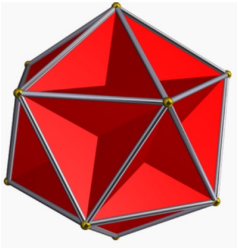
UNIVERSITA' DEGLI STUDI DELLA CAMPANIA "L.VANVITELLI"
SCUOLA POLITECNICA E DELLE SCIENZE DI BASE
DIPARTIMENTO DI MATEMATICA E FISICA
CORSO DI LAUREA IN MATEMATICA

LEZIONI DEL CORSO DI
CODICI LINEARI

FRANCESCO MAZZOCCA



Anno Accademico 2016/2017

INDICE

INDICE

INDICE

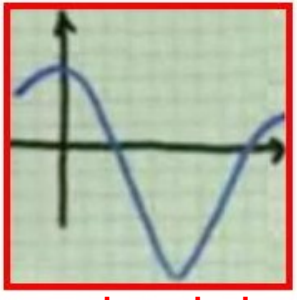
PARTE 1

SISTEMI DI COMUNICAZIONE E CODICI

1. Introduzione

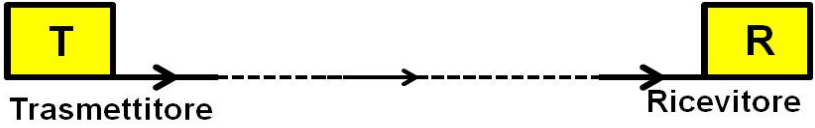
indice

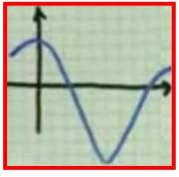
Un segnale analogico può essere intuitivamente definito come una funzione continua in un fissato intervallo di tempo



segnale analogico

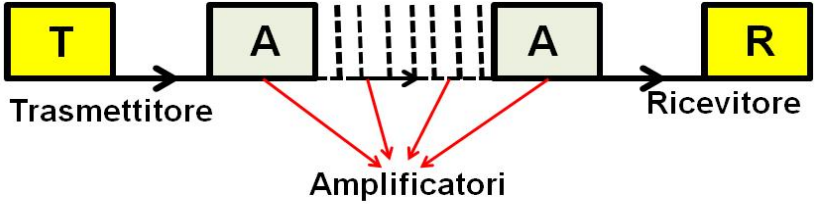
Trasmissione di un segnale analogico

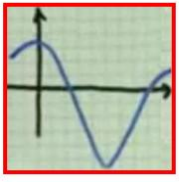




Segnale da trasmettere

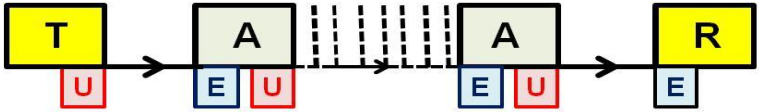
Trasmissione di un segnale analogico

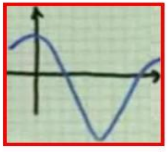




Segnale da trasmettere

Trasmissione di un segnale analogico

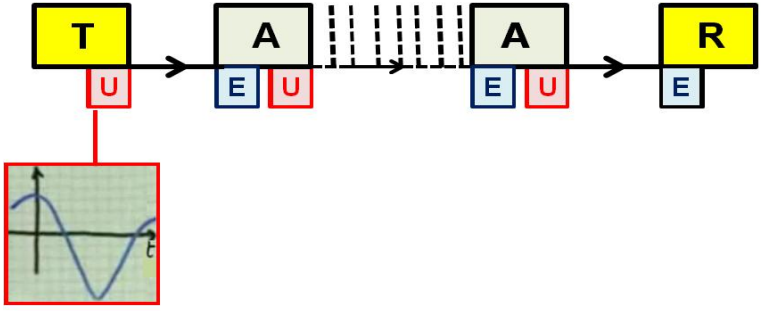




Segnale da trasmettere

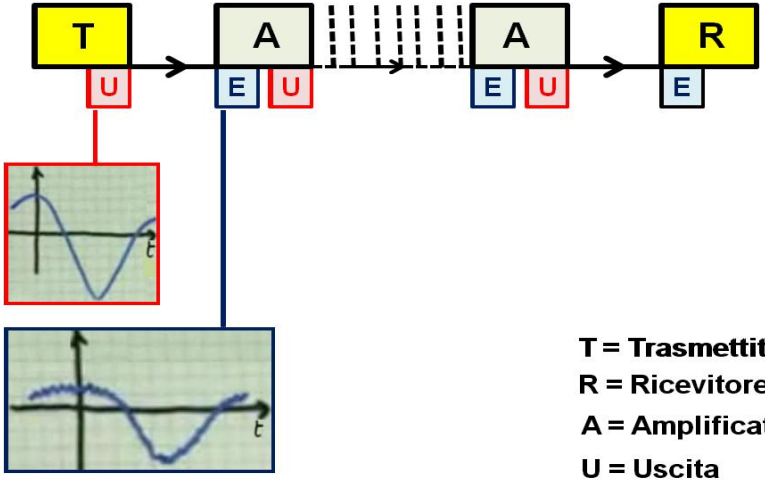
T = Trasmettitore
R = Ricevitore
A = Amplificatore
U = Uscita
E = Entrata

Trasmissione di un segnale analogico



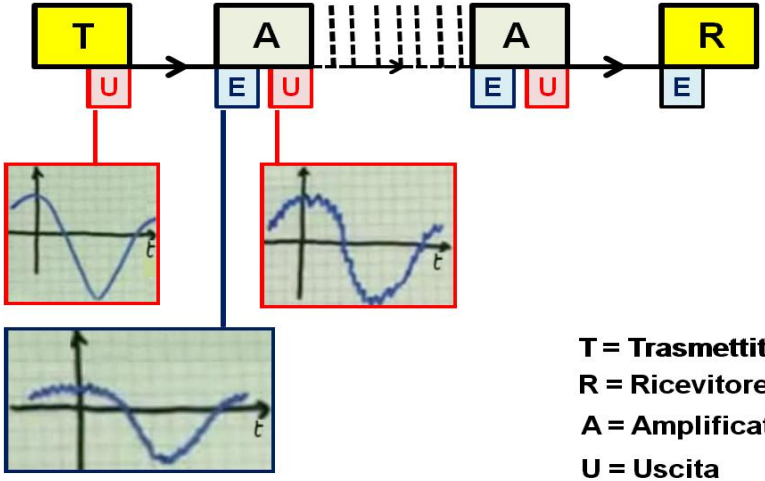
T = Trasmettitore
R = Ricevitore
A = Amplificatore
U = Uscita
E = Entrata

Trasmissione di un segnale analogico



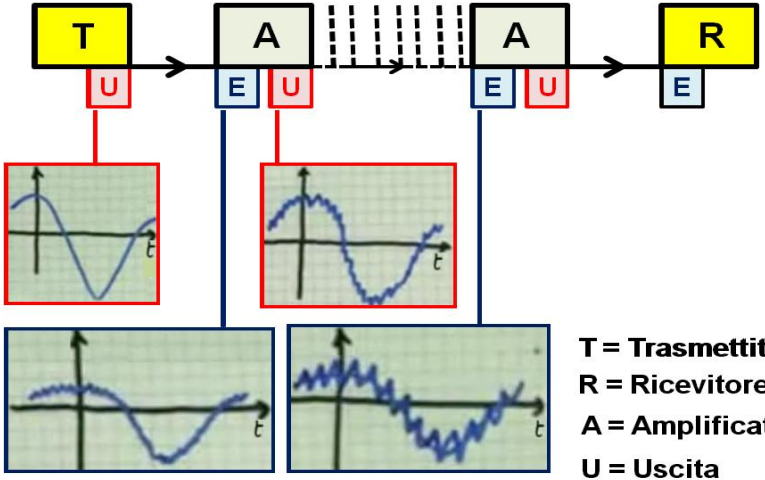
T = Trasmettitore
R = Ricevitore
A = Amplificatore
U = Uscita
E = Entrata

Trasmissione di un segnale analogico



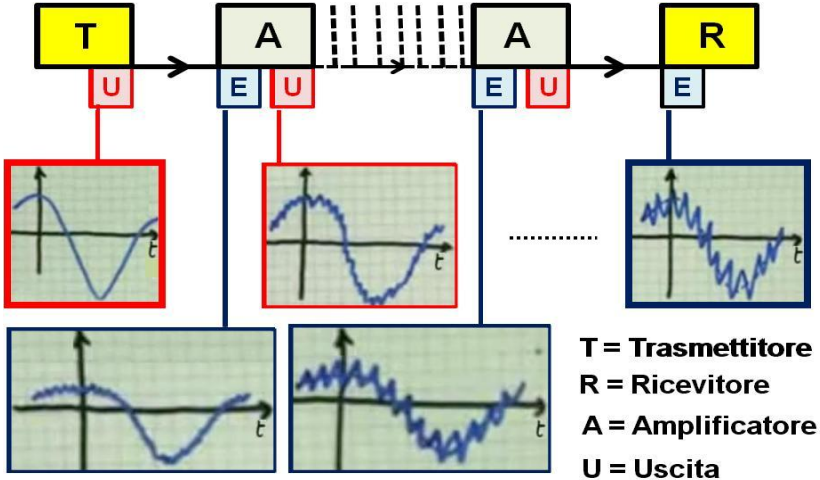
T = Trasmettitore
R = Ricevitore
A = Amplificatore
U = Uscita
E = Entrata

Trasmissione di un segnale analogico

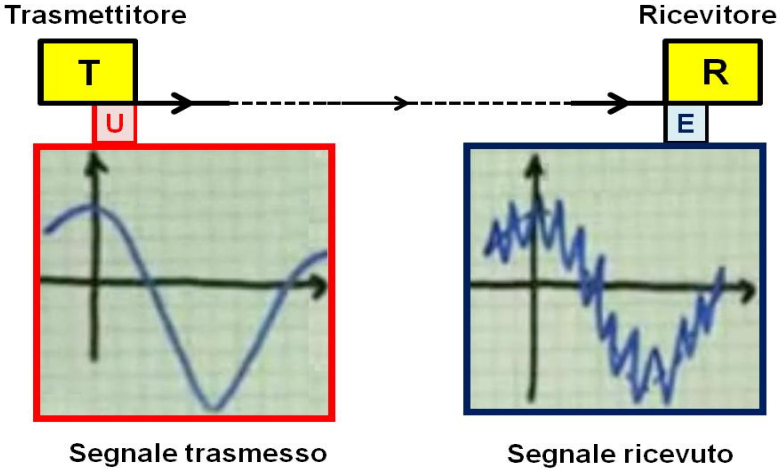


T = Trasmettitore
R = Ricevitore
A = Amplificatore
U = Uscita
E = Entrata

Trasmissione di un segnale analogico



Trasmissione di un segnale analogico

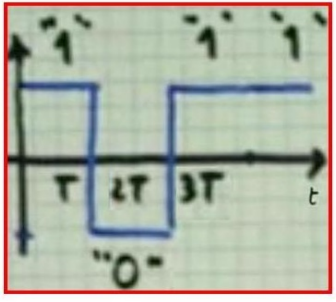


Un segnale digitale può essere intuitivamente definito come una funzione su un insieme discreto in un fissato intervallo di tempo

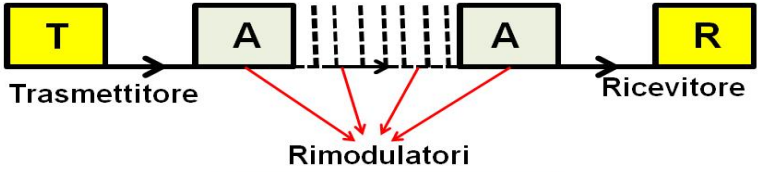
segnale digitale (binario)

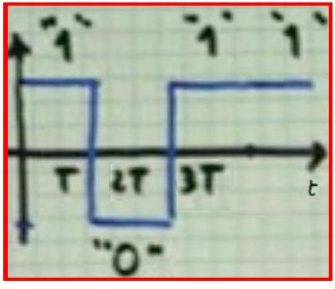
Trasmissione di un segnale digitale (numerico)

Segnale da trasmettere: **1011**



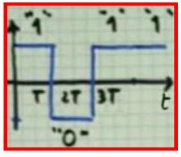
Trasmissione di un segnale digitale (numerico)





Segnale da trasmettere

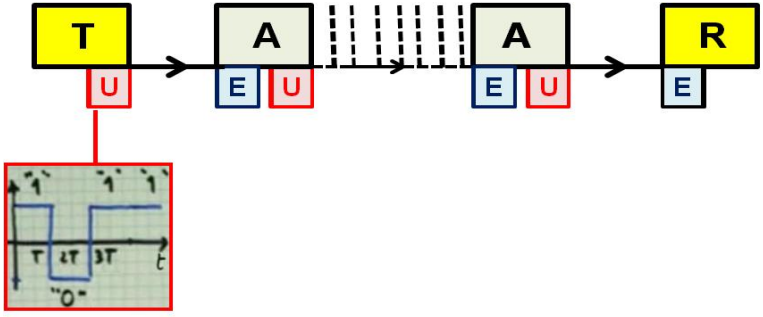
Trasmissione di un segnale digitale (numerico)



Segnale da trasmettere

T = Trasmettitore
R = Ricevitore
A = Rimodulatore
U = Uscita
E = Entrata

Trasmissione di un segnale digitale (numerico)



T = Trasmettitore

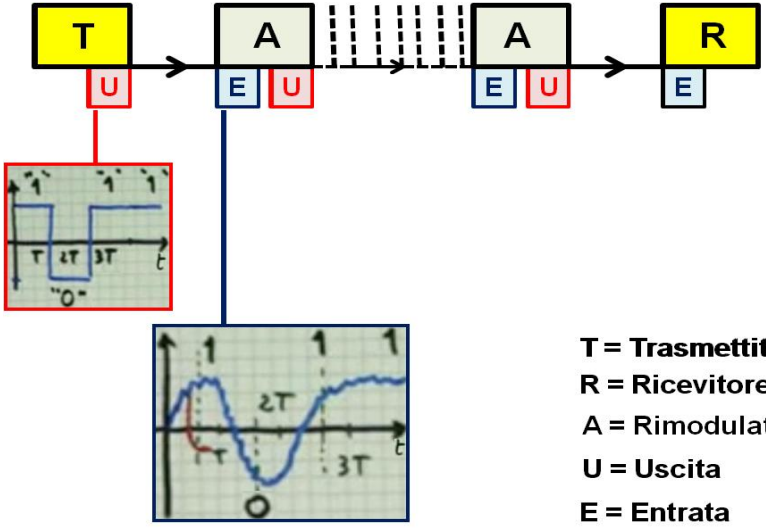
R = Ricevitore

A = Rimodulatore

U = Uscita

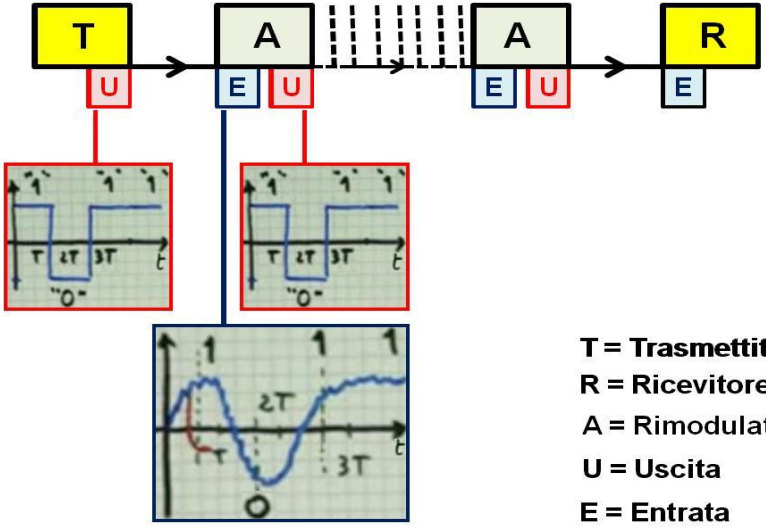
E = Entrata

Trasmissione di un segnale digitale (numerico)



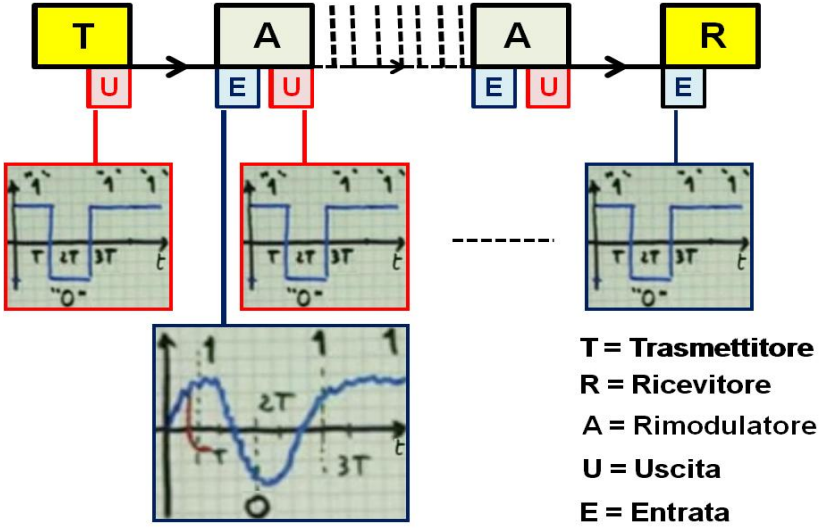
T = Trasmettitore
R = Ricevitore
A = Rimodulatore
U = Uscita
E = Entrata

Trasmissione di un segnale digitale (numerico)

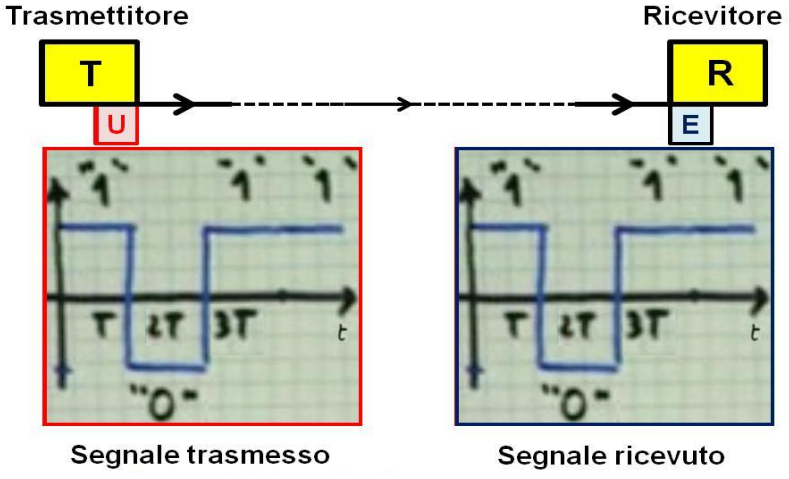


T = Trasmettitore
R = Ricevitore
A = Rimodulatore
U = Uscita
E = Entrata

Trasmissione di un segnale digitale (numerico)



Trasmissione di un segnale digitale (numerico) in assenza di errori



Alcuni dei motivi che hanno definitivamente segnato la vittoria del digitale sull'analogico

Relativamente all'harware e alle moderne tecnologie:

- **fedeltà** nella trasmissione del segnale (*rigenerazione*);
- **unificazione** del formato dei segnali (*commutazione*) nella rete ISDN;
- **potenza** ed **economicità** dei circuiti numerici VLSI.

Relativamente al software (**interessante per noi!**):

- possibilità di **riduzione della ridondanza** della sorgente di informazione e di **correzione degli errori** in ricezione.

Una situazione imbarazzante!

(O.Pretzel, *Error-Correcting Codes and Finite Fields*, 1992)

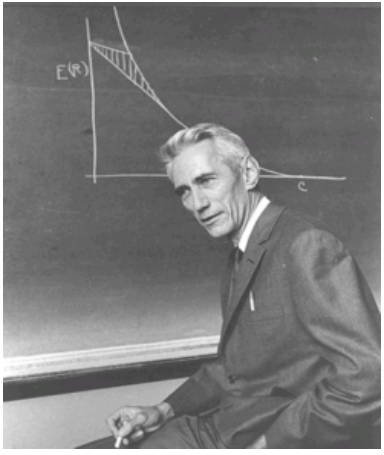
"Ti svegli una mattina, e nella semioscurità vedi una figura con uno strano cappello accucciata in un angolo della stanza. Dopo un pò i tuoi occhi focalizzano e ti accorgi che in realtà sono i tuoi vestiti buttati su una sedia.
Noti poi che la tua amata se n'è andata e trovi un biglietto sul cuscino che dice "I LOVE XOU".
Quasi certamente questo ti rassicurerà, perché presumerai che nel buio la Y sembri una X. Certo, non sei sicuro al 100 %. Potrebbe anche essere che in realtà la X sia una L e che sei stato abbandonato per il tuo caro amico (o almeno così credevi) Lou."

Quando riceviamo un'informazione non possiamo fidarci delle apparenze.

Dobbiamo sempre verificare che l'informazione ricevuta corrisponda esattamente a quella che è stata inviata.

Claude Shannon

Il fondatore della Teoria dell'Informazione



30.04.1916 (Gaylord, Michigan, USA)
24.02.2001 (Medford, Massachusetts, USA)

`http://www-history.mcs.st-and.ac.uk/Biographies/Shannon.html`

Nascita della teoria dell'informazione

http://worrydream.com/refs/Shannon-AMathematicalTheoryofCommunication.pdf

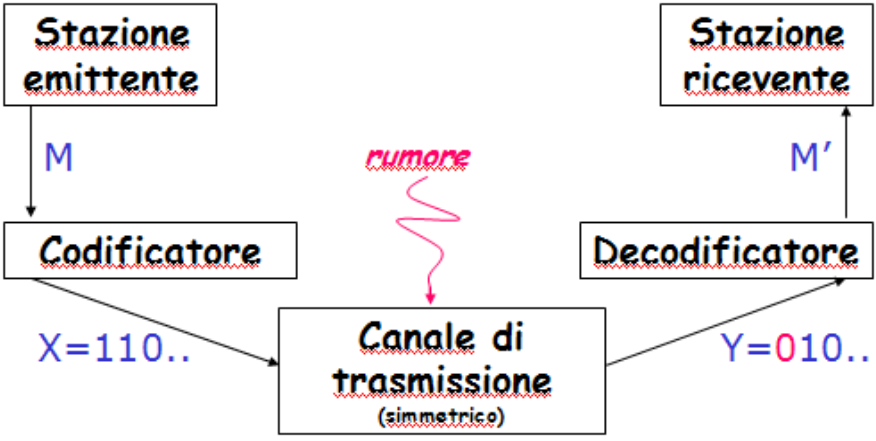
L'articolo di *Claude Elwood Shannon*

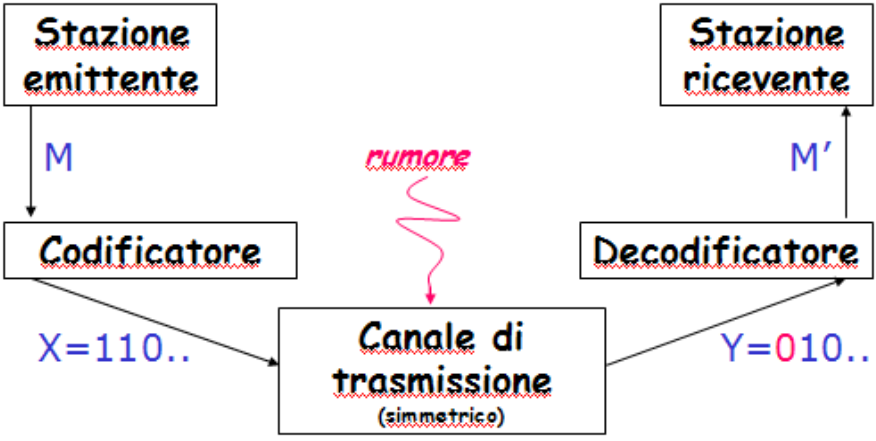
A Mathematical Theory of Communication
The Bell System Techical Journal,
Vol.27, pp379-656, July, October, 1948

segna l'inizio della Teoria dell'Informazione.
Qui per la prima volta si traduce in termini matematici precisi ciò che comunemente si intende per *informazione*. È, inoltre, precisato il problema fondamentale della comunicazione:

The fundamental problem of communication
is that of reproducing at one point
either exactly or approximately
a message selected at another point.

Questo significa che da un *messaggio ricevuto*, anche se in errore, deve potersi risalire al *messaggio inviato*.


Stazione emittente
Stazione ricevente
M
rumore
M'
Codificatore
Decodificatore
X=110..
Canale di trasmissione
(simmetrico)
Y=010..



PROBLEMA

Fare in modo che sia $M=M'$

Un risultato fondamentale

Uno dei risultati (teorici) fondamentali di Shannon può sintetizzarsi nel modo seguente:

Si può sempre comunicare in modo efficiente a patto di liberare prima il messaggio da tutta l'informazione in eccesso (compressione dei dati) e di aggiungere poi in modo controllato altra informazione (ridondanza) che permetta di scoprire o correggere eventuali errori dipendenti dalla trasmissione.

La *compressione di dati* e l'*aggiunta di ridondanza controllata* costituiscono due problemi che possono essere studiati usando dei modelli matematici.
La *teoria dei codici lineari* è particolarmente utile allo studio del secondo problema.

Un esempio di ridondanza della lingua italiana

Sneocdo uno sdtiuo dlel'Untisverà di Cabmbrige, non irmptoa cmoe snoo sctrite le plaroe, tutte le letetre posnsoo esesre al pstoo sbgalaito, è ipmtortane sloo che la prmia e l'umiltia letrtea saino al ptoso gtsiuo, il rteso non ctona, il cerlvelo è comquune semrpe in gdrao di decraifre tttuo qtueso coas, pcheré non lgege ongi silngoa ltetrea, ma lgege la palroa nel suo insmiee...

Esempio: trasmissione di un messaggio scelto tra *SI* e *NO*

COMPRESSIONE DI DATI

Se poniamo

$$SI = 1 \qquad \textbf{e} \qquad NO = 0$$

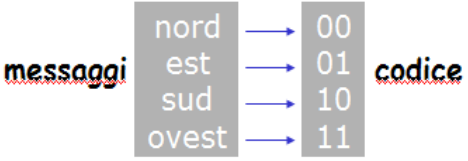
riduciamo al minimo possibile i simboli (e quindi l'informazione) che servono per trasmettere le parole *SI* e *NO*.
In tal modo, un errore sul simbolo 0 o sul simbolo 1 altera completamente il messaggio perché trasforma *NO* in *SI* e *SI* in *NO*.
Questa codifica non è buona per una trasmissione sicura su un canale che "ogni tanto" produce un errore.

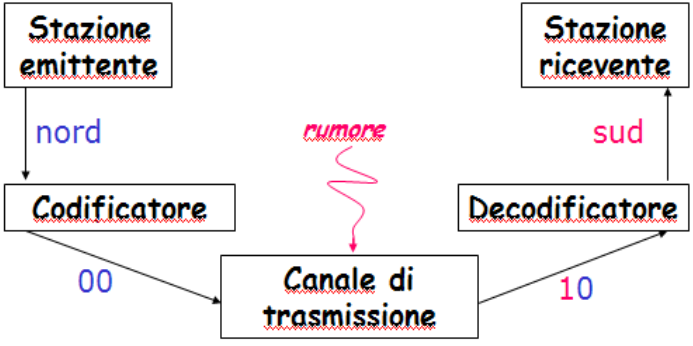
AGGIUNTA DI RIDONDANZA A DATI COMPRESSI

Se abbiamo un canale che può andare in errore al più una volta ogni tre simboli trasmessi, allora:
- la codifica $SI = 11$ e $NO = 00$ permette di *scoprire* un errore;
- la codifica $SI = 111$ e $NO = 000$ permette di *correggere* un errore.

Trasmissione su un canale che commette al più un errore ogni 5 bit

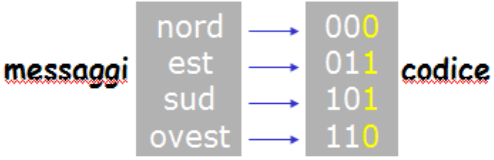
con codice senza ridondanza

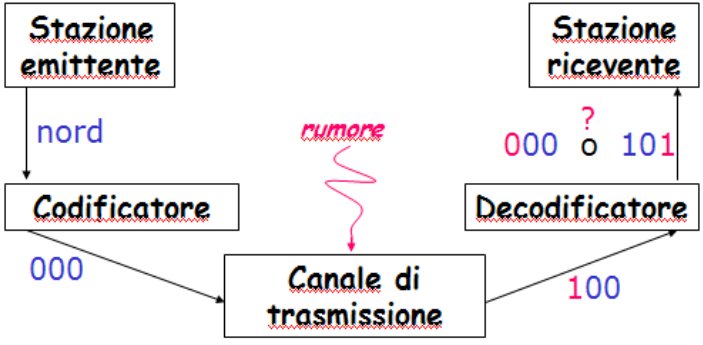




Trasmissione su un canale che commette al più un errore ogni 5 bit

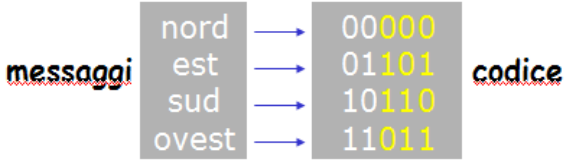
con codice ridondante che scopre un errore

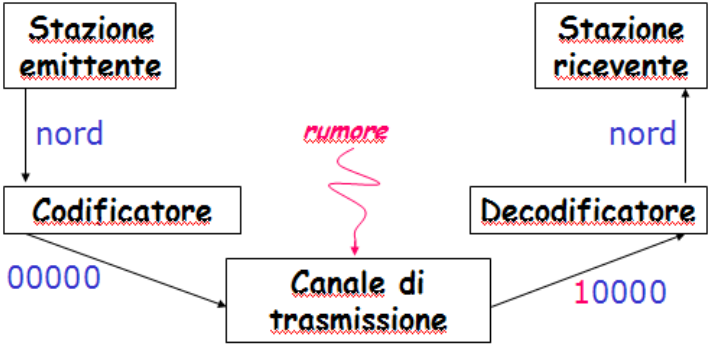




Trasmissione su un canale che commette al più un errore ogni 5 bit

con codice ridondante che corregge un errore





La dimostrazione del teorema di Shannon non è di tipo costruttivo e non si conoscono metodi generali per la costruzione di codici ”efficienti” per la trasmissione dell'informazione attraverso un prefissato canale.
Richard W.Hamming è stato un pioniere nella ricerca di tali codici.

11.02.1915 (Chicago, Illinois, USA)
07.01.1998 (Monterey, California, USA)
http:
//www-history.mcs.st-and.ac.uk/Biographies/Hamming.html

Self-Correcting Codes
Case 20878, Memorandum 1130-RWH-MFW,
Bell Telephone (1947)
di R.W.Hamming

Qui viene descritta per la prima volta una classe di codici che riescono ad autocorreggere un errore.

I dati (cioè le informazioni) sono rappresentati dalle successioni binarie di lunghezza t^2.
Ogni dato è codificato da una successione binaria di lunghezza $(t+1)^2$; si aggiungono cioè $2t+1$ simboli di controllo.
Per codificare un dato si opera nel seguente modo:
• si dispongono gli elementi di una successione binaria di lunghezza t^2 in una matrice quadrata d'ordine t,
• si orla tale matrice con le somme modulo 2 degli elementi di ciascuna linea e, per ultimo, si aggiunge la somma modulo 2 di tutti gli elementi della matrice di partenza.
• La successione di lunghezza $(t+1)^2$ ottenuta scrivendo di seguito le righe della nuova matrice sarà la codifica del dato di partenza.

Esempio

Nel caso $t = 3$, per la codifica del dato 010011100, dobbiamo formare la matrice

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

e orlarla con la somma modulo 2 delle sue linee e di tutti i suoi elementi

$$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \tag{1}$$

La codifica cercata è: 010101101001101 0 , ove sono denotate in rosso le cifre di controllo aggiunte al dato di partenza.
È chiaro che, se nella (1) si cambia valore in un posto, ricalcolando i controlli si individua il posto in cui è stato cambiato il valore iniziale: il nostro codice autocorregge un errore!

2. Codici

indice

Alfabeti e parole

DEFINIZIONE 1

Un insieme finito F con q elementi prende il nome di *alfabeto finito con q lettere*, le *lettere* essendo gli elementi di F.

DEFINIZIONE 2

Una *parola di lunghezza n su un alfabeto F* è una successione finita

$$a_1 a_2 \ldots a_n$$

di lettere di F.

ESEMPIO 3

Sia F l'alfabeto della lingua italiana. Le successioni

agdter, vvvnhwe, tavolo, vovovl, sala, aula

sono esempi di parole su F. Si noti che una parola su F può non avere significato nella lingua italiana.

Convenzione

Spesso, per comodità di scrittura, identificheremo una parola $a_1 a_2 \dots a_n$ con l'$n-$pla corrispondente $\boldsymbol{a} = (a_1, a_2, ..., a_n)$.
Una parola di lunghezza n sarà, così, considerata come un elemento di F^n.

OSSERVAZIONE 4

Se l'alfabeto F è un campo, una parola di lunghezza n sarà un vettore dello spazio vettoriale F^n.

DEFINIZIONE 5

Un *codice* C su un alfabeto F è un qualsiasi sottoinsieme finito e non vuoto di parole su F.
Un codice si dice *a blocchi* se le sue parole hanno tutte la stessa lunghezza; nel caso contrario si dice *a lunghezza variabile*. La comune lunghezza delle parole di un codice a blocchi si chiama *lunghezza del codice*.

ESEMPIO 6

Sia F l'alfabeto della lingua italiana. L'insieme delle parole della lingua italiana sono un esempio di codice (a lunghezza variabile) su F.

DEFINIZIONE 7

Un codice su un alfabeto con q lettere che contenga esattamente M parole di lunghezza n prende il nome di $(n, M)-$*codice* $q-$*ario*, o semplicemente di $(n, M)-$*codice*, se q risulta chiaro dal contesto.

Nei casi $q = 2, 3$ il codice si dice rispettivamente *binario* e *ternario*.

DEFINIZIONE 8

Per un $(n, M)-$codice $q-$ario C, il numero reale

$$R(C) = \frac{\log_q M}{n}$$

prende il nome di *tasso di informazione* di C.

$$R(C) = \frac{\log_q M}{n}$$

- Il tasso di informazione di C è massimo, cioè uguale a 1, quando $M = q^n$. In questo caso C coincide con l'insieme F^n di tutte le parole su F di lunghezza n e non ha alcuna ridondanza. Questo significa che se si cambia anche una sola lettera in una parola di C si ottiene ancora una parola di C e, di conseguenza, C non può rilevare o correggere errori.

- Il tasso di informazione di C è minimo, cioè uguale a 0, quando C consta di una sola parola.

- Per il codice $C = \{(a, a, \cdots, a) \in F^n \ con \ a \in F\}$ (codice di ripetizione $q-$ario di lunghezza n) si ha $R(C) = \frac{1}{n}$. Questo tasso tende a 0 al tendere di n all'infinito.

Il Codice Fiscale Italiano

Il Codice Fiscale Italiano

È un codice su un alfabeto di 36 lettere (le 26 dell'alfabeto inglese e le cifre decimali da 0 a 9).

Serve a codificare qualunque persona o ente abbia rapporti con il sistema fiscale italiano.

Nel caso di una persona fisica la parola corrispondente è composta da 16 lettere:
- le prime 6 si riferiscono a cognome e nome,
- il secondo gruppo di 5 individua la data di nascita e il sesso,
- il successivo gruppo di 4 individua la località italiana o lo stato estero di nascita,
- l'ultima, che è di *controllo,* si calcola mediante un opportuno algoritmo sulle prime 15.

Per maggiori informazioni si veda la seguente pagina web:

http://it.wikipedia.org/wiki/Codice_fiscale

Il codice *ISBN*

International Standard Book Number

Il codice *ISBN*

International Standard Book Number (https://it.wikipedia.org/wiki/ISBN)

È un codice a blocchi C di lunghezza 10 sull'alfabeto di undici lettere costituite dalle cifre decimali da 0 a 9 e dalla lettera X.

È usato per codificare i libri in commercio.
Lo schema di codifica, ad esempio, di un libro scritto in inglese è il seguente:
- la prima lettera a_1 di una parola $\boldsymbol{a}$ è zero e corrisponde alla lingua inglese;
- le due lettere successive a_2a_3 individuano la casa editrice;
- le sei lettere successive $a_4a_5a_6a_7a_8a_9$ indicano un numero assegnato al libro dalla casa editrice;
- l'ultima lettera a_{10} è di controllo ed è uguale al resto r della divisione per 11 dell'intero

$$a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9$$

se $0 \leq r \leq 9$, è invece uguale ad X se risulta $r = 10$.

Il codice Morse

(https://it.wikipedia.org/wiki/Codice_Morse)

È un codice (storico) a lunghezza variabile sull'alfabeto di tre lettere

$$F = \{\bullet, -, \textit{"spazio"}\}.$$

Serve a codificare le lettere dell'alfabeto inglese.

A	•–	*B*	–•••	*C*	–•–•	*D*	–••
E	•	*F*	••–•	*G*	––•	*H*	••••
I	••	*J*	•–––	*K*	–•–	*L*	•–••
M	––	*N*	–•	*O*	–––	*P*	•––•
Q	––•–	*R*	•–•	*S*	•••	*T*	–
U	••–	*V*	•••–	*W*	•––	*X*	–••–
Y	–•––	*Z*	––••				

Si osservi che una sua parola è tanto più lunga quanto la lettera corrispondente è meno frequente nella lingua inglese.

Il codice Morse

(https://it.wikipedia.org/wiki/Codice_Morse)

Quando si codifica una frase, bisogna inserire esattamente uno *"spazio"* tra ogni due lettere dell'alfabeto codificate ed almeno due spazi fra ogni due parole. Per esempio, se usiamo il simbolo "@" per indicare uno *"spazio"*, l'espressione

CODICE MORSE

si codifica con

– • – • @ – – – @ – • • @ • •@ – • – •@ • @@ – –@ – – – @ • – • @ • • • @•

Osserviamo che il codice Morse non distingue le lettere minuscole dalle maiuscole.

Il codice ASCII

American Standard Code for Information Interchange (https://it.wikipedia.org/wiki/ASCII)

È il codice a blocchi sull'alfabeto $F = \{0, 1\}$ formato da tutte le parole di lunghezza sette e, quindi, contiene esattamente $2^7 = 128$ parole.

Serve per codificare le lettere dell'alfabeto inglese maiuscole e minuscole, le cifre decimali da 0 a 9 e una serie di altri simboli e istruzioni allo scopo di permettere all'architettura interna di un computer di operare solo con i simboli 0 e 1.

CODIFICA DELLE LETTERE MAIUSCOLE DELL'ALFABETO

A	1000001	*B*	1000010	*C*	1000011	*D*	1000100
E	1000101	*F*	1000110	*G*	1000111	*H*	1001000
I	1001001	*J*	1001010	*K*	1001011	*L*	1001100
M	1001101	*N*	1001110	*O*	1001111	*P*	1010000
Q	1010001	*R*	1010010	*S*	1010011	*T*	1010100
U	1010101	*V*	1010110	*W*	1010111	*X*	1011000
Y	1011001	*Z*	1011010				

Il codice ASCII esteso

Extended American Standard Code for Information Interchange

Se ad ogni parola del codice ASCII si aggiunge 0 o 1, a seconda che contenga un numero pari o dispari di 1 rispettivamente, si ottiene un codice a blocchi di lunghezza otto, detto *codice ASCII esteso.*

CODIFICA DELLE LETTERE MAIUSCOLE DELL'ALFABETO

A	10000010	*B*	10000100	*C*	10000111	*D*	10001000
E	10001011	*F*	10001101	*G*	10001110	*H*	10010000
I	10010011	*J*	10010101	*K*	10010110	*L*	10011001
M	10011010	*N*	10011100	*O*	10011111	*P*	10100000
Q	10100011	*R*	10100101	*S*	10100110	*T*	10101001
U	10101010	*V*	10101100	*W*	10101111	*X*	10110001
Y	10110010	*Z*	10110100				

Il tasso di informazione di questo codice è

$$\frac{\log_2 2^7}{8} = \frac{7}{8} = 0,875\,.$$

Il codice EAN

European Article Number Code

È un codice a blocchi di lunghezza 13 su un alfabeto di 12 lettere (le dieci cifre decimali, un carattere di start/stop e uno di controllo centrale).
Serve per codificare mediante delle *barre* gli articoli in commercio soggetti alle cosiddette specifiche EAN (European Article Number). Il formato finale è leggibile automaticamente in entrambe le direzioni.
Vi sono 2 moduli elementari dello stesso spessore: una barra nera e uno spazio (barra bianca). Le altre barre possono assumere 4 diversi spessori, multipli interi di quello dei moduli elementari.
Ogni cifra si codifica con 7 moduli elementari, il carattere di controllo centrale con 5 e quello di start/stop con 3.
Per lo schema di codifica ed esempi si veda la seguente pagina web:

http://www.codiceabarre.it/bcean.htm

Il $(7, 16)-$codice binario di Hamming

È un codice sulle lettere $0, 1$ del campo Z_2 dei resti modulo 2.

Le sue parole sono i 16 vettori $(X_1, X_2, X_3, X_4, X_5, X_6, X_7)$ dello spazio vettoriale numerico Z_2^7 per cui risulta:

$a = X_4 + X_5 + X_6 + X_7 = 0\,,$
$b = X_2 + X_3 + X_6 + X_7 = 0\,,$
$c = X_1 + X_3 + X_5 + X_7 = 0\,.$

Si può provare che, se si cambia la componente $j-$esima di una parola del codice e, per la nuova parola, si calcolano a, b, c in Z_2, allora abc è la rappresentazione binaria dell'intero j.

Questo significa che il codice autocorregge un errore.
Il tasso di informazione di questo codice è

$$\frac{\log_2 2^4}{7} = \frac{4}{7} = 0,57142857\,.$$

Per esempio, la parola $\boldsymbol{x} = (0, 0, 1, 1, 0, 0, 1)$ appartiene al nostro codice, essendo

$a = X_4 + X_5 + X_6 + X_7 = 1 + 0 + 0 + 1 = 0\,,$
$b = X_2 + X_3 + X_6 + X_7 = 0 + 1 + 0 + 1 = 0\,,$
$c = X_1 + X_3 + X_5 + X_7 = 0 + 1 + 0 + 1 = 0\,.$

Se consideriamo la parola $(0, 0, 1, 1, 1, 0, 1)$, ottenuta da $\boldsymbol{x}$ modificando la quinta componente, e calcoliamo i rispettivi a, b, c, otteniamo

$$a = 1, b = 0, c = 1$$

e 101 è proprio la rappresentazione binaria di 5.

Il $(4, 9)-$codice ternario di Hamming

È un codice sulle lettere $0, 1, 2$ del campo Z_3 dei resti modulo 3.
Le sue parole sono i 9 vettori (X_1, X_2, X_3, X_4) dello spazio vettoriale numerico Z_3^4 per cui risulta:

$$X_1 + X_2 - X_3 = 0\,, \qquad X_2 + X_3 + X_4 = 0\,.$$

Le parole del codice sono le seguenti:

$$(0,0,0,0)\,,\ (1,0,1,2)\,,\ (2,0,2,1)\,,$$

$$(0,1,1,1)\,,\ (1,1,2,0)\,,\ (2,1,0,2)\,,$$

$$(0,2,2,2)\,,\ (1,2,0,1)\,,\ (2,2,1,0)\,.$$

È possibile provare che anche questo codice autocorregge un errore. Il suo tasso di informazione è

$$\frac{\log_3 3^2}{4} = \frac{2}{4} = 0,5\,.$$

Composizione di parole

L'insieme di tutte le parole su un alfabeto F si denota con F^*; si pone cioè

$$F^* = \bigcup_{j \in N} F^j.$$

Su F^* è definita in modo naturale una moltiplicazione associativa, detta *composizione* o *concatenazione* di parole, nel seguente modo:

$$\boldsymbol{a} = a_1 a_2 ... a_n \,,\, \boldsymbol{b} = b_1 b_2 ... b_m \in F^*,$$

$$\boldsymbol{ab} = a_1 a_2 ... a_n b_1 b_2 ... b_m$$

Quando per una parola $\boldsymbol{c}$ risulta $\boldsymbol{c} = \boldsymbol{ab}$ si dice che $\boldsymbol{a}$ è un *prefisso* di $\boldsymbol{c}$.
Ad esempio, per le parole binarie

$$\boldsymbol{a} = 100110,\ \boldsymbol{b} = 0101,\ \boldsymbol{c} = 100,\ \boldsymbol{d} = 1100,\ \boldsymbol{e} = 101,$$

risulta $\boldsymbol{ab} = 1001100101 = \boldsymbol{cde}\,, \boldsymbol{cd} = 1001100$. Si osservi che le parole $\boldsymbol{c}$ e $\boldsymbol{cd}$ sono prefissi della parola $\boldsymbol{ab}$.

Codici decifrabili

DEFINIZIONE 9

Il prodotto di un numero finito di parole di un codice C prende il nome di *stringa di C* o, più semplicemente *stringa*, se il codice C è individuato dal contesto.

DEFINIZIONE 10

Un codice C si dice *decifrabile* se vale la seguente proprietà: *due stringhe di C*

$$\boldsymbol{a} = \boldsymbol{a}_1\boldsymbol{a}_2\cdots\boldsymbol{a}_h,\ \ \boldsymbol{b} = \boldsymbol{b}_1\boldsymbol{b}_2\cdots\boldsymbol{b}_k,$$

sono uguali se, e solo se, risulta

$$h = k \ \ e \ \ \boldsymbol{a}_1 = \boldsymbol{b}_1,\, \boldsymbol{a}_2 = \boldsymbol{b}_2, \ldots, \boldsymbol{a}_h = \boldsymbol{b}_h\,.$$

OSSERVAZIONE 11

Un codice decifrabile C garantisce che, leggendo (da sinistra a destra) le lettere di una sua stringa, è possibile riconoscere senza ambiguità tutte le sue parole che, nell'ordine, formano la stringa data.

ESEMPIO 12

Il codice

$$C_1 = \{\boldsymbol{a} = 0,\ \boldsymbol{b} = 01,\ \boldsymbol{c} = 001\}$$

non è decifrabile perché risulta $\boldsymbol{c} = \boldsymbol{ab}$.

ESEMPIO 13

Il codice

$$C_2 = \{\boldsymbol{a} = 1,\ \boldsymbol{b} = 10,\ \boldsymbol{c} = 100\}$$

è decifrabile. Notiamo che, se sappiamo che una stringa del codice C_2 inizia con con 10, non siamo in grado di decidere se la prima parola della stringa è 10 oppure 100, come mostrano le seguenti stringhe

$$10 \cdot 100 \cdot 1 \cdot 1 \cdot 1 \cdot 100 \quad \text{e} \quad 100 \cdot 100 \cdot 10 \cdot 10\,,$$

ove, separandole con un puntino, abbiamo messo in evidenza le parole di C_2 che formano le stringhe.

OSSERVAZIONE 14

Il codice $C_2 = \{\boldsymbol{a} = 1, \boldsymbol{b} = 10, \boldsymbol{c} = 100\}$ mostra un inconveniente di alcuni codici decifrabili: *per riconoscere le parole del codice che formano una stringa, bisogna conoscere l'intera stringa*.

DEFINIZIONE 15

Si dice che un codice C è *istantaneo*, o che ha la proprietà del prefisso, se nessuna delle sue parole è prefisso di un'altra parola di C.

OSSERVAZIONE 16

Ogni codice istantaneo è anche decifrabile. Esistono, invece, codici decifrabili e non istantanei, come il codice C_2 dell'Esempio 13.

ESEMPIO 17

Il codice

$$C_3 = \{a = 1,\ b = 01,\ c = 001\}$$

è istantaneo. I codici a blocchi sono istantanei.

OSSERVAZIONE 18

Un codice istantaneo C garantisce che, leggendo (da sinistra a destra) le lettere di una sua stringa, appena si riconosce una parola di C, questa è necessariamente una delle sue parole che formano la stringa data (*decodifica istantanea*, o *online*).

ESEMPIO 19

Se una stringa del codice C_3 è del tipo

1100101.....

allora nella stringa in questione si ha senza possibilità di equivoci che le parole iniziali sono nell'ordine 1, 1, 001, 01.

Il teorema di Kraft

Sia C un codice q−ario (su un alfabeto F) costituito dalle M parole $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_M$ *di rispettive lunghezze* $\ell_1, \ell_2, \ldots, \ell_M$. *Allora, se C è istantaneo, vale la seguente disuguaglianza*

$$\sum_{j=1}^{M} \frac{1}{q^{\ell_j}} \leq 1 \qquad \textbf{(Disuguaglianza di Kraft)}. \tag{2}$$

Inoltre, se $M+1$ *interi positivi* $\ell_1, \ell_2, \ldots, \ell_M, q$ *verificano la disuguaglianza* (2), *allora esiste un codice istantaneo q−ario con M parole di lunghezza* $\ell_1, \ell_2, \ldots, \ell_M$, *rispettivamente.*

ESEMPIO 20

Il codice $C_4 = \{\boldsymbol{a} = 0,\ \boldsymbol{b} = 11,\ \boldsymbol{c} = 100,\ \boldsymbol{d} = 110\}$ verifica la disuguaglianza di Kraft perché risulta

$$\frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^3} = 1\,.$$

Ciò nonostante il codice non è istantaneo perché risulta $\boldsymbol{d} = \boldsymbol{ba}$.

Dimostrazione del teorema di Kraft

Prima parte

- Sia L il massimo delle lunghezze delle parole del codice C.
- Per ogni $\boldsymbol{a}_j \in C$, consideriamo l'insieme A_j delle parole su F di lunghezza L che hanno $\boldsymbol{a}_j$ come prefisso.
- Ogni A_j contiene esattamente $q^{L-\ell_j}$ parole e nessuna di queste appartiene a C(una parola di C non può avere come prefisso un'altra parola di C!).
- Ne segue che l'intero

$$\sum_{j=1}^{M} q^{L-\ell_j} = \sum_{j=1}^{M} \frac{q^L}{q^{\ell_j}}$$

è il numero di tutte le parole di lunghezza L aventi come prefisso una parola di C.

- Questo numero non può superare il numero q^L di tutte le parole di lunghezza L e, quindi abbiamo

$$\sum_{j=1}^{M} \frac{q^L}{q^{\ell_j}} \leq q^L \;\Rightarrow\; \sum_{j=1}^{M} \frac{1}{q^{\ell_j}} \leq 1\,.$$

- Ricordando che abbiamo posto $L = max_{j=1}^{M} \ell_j$, denotiamo con m_t il numero di interi ℓ_j uguali a t, per ogni $t = 1, 2, \ldots, L$.
- Abbiamo

$$\sum_{j=1}^{M} \frac{1}{q^{\ell_j}} \leq 1 \;\Rightarrow\; \sum_{j=1}^{M} \frac{1}{q^{\ell_j}} = \frac{m_1}{q} + \frac{m_2}{q^2} + \cdots + \frac{m_L}{q^L} \leq 1\,,$$

da cui, moltiplicando per q^L,

$$m_L \leq q^L - m_1 q^{L-1} - m_2 q^{L-2} - \cdots - m_{L-1} q$$

e, essendo $m_L \geq 1$,

$$m_{L-1} \leq q^{L-1} - m_1 q^{L-2} - m_2 q^{L-3} - \cdots - m_{L-2} q\,.$$

Dimostrazione del teorema di Kraft

Seconda parte

- Tenendo presente che per ogni t è $m_t \geq 1$, otteniamo le disuguaglianze

$$
\begin{aligned}
m_L &\leq q^L - m_1 q^{L-1} - m_2 q^{L-2} - \cdots - m_{L-1} q \\
m_{L-1} &\leq q^{L-1} - m_1 q^{L-2} - m_2 q^{L-3} - \cdots - m_{L-2} q \\
m_{L-2} &\leq q^{L-2} - m_1 q^{L-3} - m_2 q^{L-4} - \cdots - m_{L-3} q \\
&\vdots \\
m_k &\leq q^k - m_1 q^{k-1} - m_2 q^{k-2} - \cdots - m_{k-1} q \quad . \\
&\vdots \\
m_3 &\leq q^3 - m_1 q^2 - m_2 q \\
m_2 &\leq q^2 - m_1 q \\
m_1 &\leq q
\end{aligned}
$$

• A questo punto possiamo costruire il nostro codice C facendo induzione su L (algoritmo di Kraft):
1. Se $L = 1$, (i.e. il codice dovrà avere $M = m_1$ parole di lunghezza 1) per ottenere C, basta scegliere M lettere distinte nell'alfabeto F.
2. Supponiamo di aver costruito un codice istantaneo C_{k-1} avente m_t parole di lunghezza t, con $t = 1, 2, \ldots, k-1$ e osserviamo che esistono

$$q^k - m_1 q^{k-1} - m_2 q^{k-2} - \cdots - m_{k-1} q$$

parole su F di lunghezza k non aventi come prefisso una parola di C_{k-1}. Allora, avendo provato che è

$$m_k \leq q^k - m_1 q^{k-1} - m_2 q^{k-2} - \cdots - m_{k-1} q\,,$$

possiamo trovare m_k parole di lunghezza k che non hanno come prefisso una parola di C_{k-1}. Queste, aggiunte a quelle di C_{k-1}, danno luogo ad un codice istantaneo C_k avente m_t parole di lunghezza t, con $t = 1, 2, \ldots, k$.

Costruire un codice istantaneo $C = \{a_1, a_2, ..., a_6\}$ *sull'alfabeto* $\{a, b, c\}$ *con* 6 *parole di lunghezza, rispettivamente,* $\ell_1 = \ell_2 = 1$ $\ell_3 = 2$, $\ell_4 = \ell_5 = 4$, $\ell_6 = 5$.

SOLUZIONE: Osserviamo che un tale codice esiste perché vale la disuguaglianza di Kraft: $\frac{1}{3} + \frac{1}{3} + \frac{1}{3^2} + \frac{1}{3^4} + \frac{1}{3^4} + \frac{1}{3^5} = \frac{196}{243} \leq 1$.
Ora, costruiamo C :
passo 1. Per a_1 e a_2 scegliamo due lettere dell'alfabeto. Per esempio $a_1 = a$, $a_2 = b$.
passo 2. Per a_3 scegliamo una parola di lunghezza due che non abbia come prefisso a o b. Per esempio $a_3 = cb$.
passo 3. Per a_4 e a_5 scegliamo due parole di lunghezza quattro che non abbiano come prefisso $a_1 = a$, $a_2 = b$ o $a_3 = cb$. Per esempio $a_4 = caaa$, $a_5 = caba$.
passo 4. Per a_6 scegliamo una parola di lunghezza due che non abbia come prefisso nessuna delle parole già scelte. Per esempio $a_6 = cabba$.
fine algoritmo. $C = \{a, b, cb, caaa, caba, cabba\}$.

PROPOSIZIONE 21

Se $M+1$ interi positivi $\ell_1, \ell_2, \ldots, \ell_M, q$ verificano la disuguaglianza di Kraft (2), allora esiste un codice decifrabile $q-$ario con M parole di rispettive lunghezze $\ell_1, \ell_2, \ldots, \ell_M$.

DIMOSTRAZIONE

Basta ricordare che ogni codice istantaneo è decifrabile.

OSSERVAZIONE 22

La disuguaglianza di Kraft vale anche per i codici decifrabili (teorema di McMillan); ma la sua dimostrazione è più riposta e meno intuitiva di quella esposta per i codici istantanei.

Sia C un codice q−ario, su un alfabeto F, costituito dalle M parole $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_M$ *di rispettive lunghezze* $\ell_1, \ell_2, \ldots, \ell_M$. *Allora, se C è decifrabile, vale la disuguaglianza di Kraft*

$$\sum_{j=1}^{M} \frac{1}{q^{\ell_j}} \leq 1 \,.$$

ESEMPIO 23

il codice

$$C_5 = \{\boldsymbol{a} = 0,\, \boldsymbol{b} = 1,\, \boldsymbol{c} = 00,\, \boldsymbol{d} = 01,\, \boldsymbol{e} = 10,\, \boldsymbol{f} = 11\}$$

non è decifrabile perché non verifica la disuguaglianza di Kraft:

$$\frac{1}{2} + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^2} + \frac{1}{2^2} + \frac{1}{2^2} = 2 > 1 \,.$$

Dimostrazione del teorema di McMillan

- Poniamo $L = max_{j=1}^{M} \ell_j$,
- Se denotiamo con m_t il numero di interi ℓ_j uguali a t, per ogni $t = 1, 2, \ldots, L$, abbiamo

$$\sum_{j=1}^{M} \frac{1}{q^{\ell_j}} = \sum_{i=1}^{L} \frac{m_i}{q^i}$$

e, per ogni intero positivo n, risulta

$$\left(\sum_{i=1}^{L} \frac{m_i}{q^i} \right)^n = \left(\frac{m_1}{q} + \frac{m_2}{q^2} + \cdots + \frac{m_L}{q^L} \right)^n$$

$$= \sum_{1 \le i_1 < i_2 < \cdots < i_n \le L} \frac{m_{i_1}}{q^{i_1}} \frac{m_{i_2}}{q^{i_2}} \cdots \frac{m_{i_n}}{q^{i_n}} = \sum_{1 \le i_1 < i_2 < \cdots < i_n \le L} \frac{m_{i_1} m_{i_2} \cdots m_{i_n}}{q^{i_1 + i_2 + \cdots + i_n}}$$

$$= \sum_{k=n}^{nL} \left(\sum_{\substack{1 \le i_1 < i_2 < \cdots < i_n \le L \\ i_1 + i_2 + \cdots + i_n = k}} m_{i_1} m_{i_2} \cdots m_{i_n} \right) \frac{1}{q^k} = \sum_{k=n}^{nL} \frac{M_k}{q^k} \text{ , con}$$

$$M_k = \sum_{\substack{1 \le i_1 < i_2 < \cdots < i_n \le L \\ i_1 + i_2 + \cdots + i_n = k}} m_{i_1} m_{i_2} \cdots m_{i_n} .$$

Dimostrazione del teorema di McMillan

- Poiché C è decifrabile, l'intero

$$m_{i_1} m_{i_2} \cdots m_{i_n},$$

con $i_1 + i_2 + \cdots + i_n = k$, è esattamente il numero di stringhe di C di lunghezza k del tipo $\boldsymbol{a}_{i_1} \boldsymbol{a}_{i_2} \cdots \boldsymbol{a}_{i_n}$, ove $\boldsymbol{a}_{i_s}$ è una parola di C di lunghezza i_s, per ogni $s = 1, 2, ..., n$.

- Ne segue che M_k è esattamente il numero delle stringhe di C di lunghezza k che possono ottenersi componendo n parole di C. D'altra parte il numero di tutte le parole su F di lunghezza k è esattamente q^k, quindi $M_k \leq q^k$ e

$$\left(\sum_{i=1}^{L} \frac{m_i}{q^i} \right)^n = \sum_{k=n}^{nL} \frac{M_k}{q^k} \leq \sum_{k=n}^{nL} 1 \leq nL.$$

Dimostrazione del teorema di McMillan

- Allora, elevando a $\frac{1}{n}$ primo e secondo membro della disuguaglianza

$$\left(\sum_{i=1}^{L} \frac{m_i}{q^i} \right)^n \leq nL \,,$$

si ottiene

$$\sum_{i=1}^{L} \frac{m_i}{q^i} \leq n^{1/n} L^{1/n}$$

e, facendo tendere n all'infinito, otteniamo

$$\sum_{i=1}^{L} \frac{m_i}{q^i} \leq 1 \,.$$

PROPOSIZIONE 24

Se esiste un codice $q-$ario decifrabile C con M parole di lunghezza ℓ_1, ℓ_2,...,ℓ_M, allora esiste anche un codice C' istantaneo con parole della stessa lunghezza.

DIMOSTRAZIONE

Per il teorema di McMillan gli interi $\ell_1, \ell_2, ..., \ell_M, q$ verificano la disuguaglianza di Kraft e, allora, il codice C' esiste in forza del teorema di Kraft.

OSSERVAZIONE 25

I risultati di questo paragrafo ci danno informazioni sul "prezzo che dobbiamo pagare" se vogliamo un codice decifrabile: le lunghezze ℓ_i delle parole devono essere "*abbastanza" grandi affiché i numeri* $1/q^{\ell_i}$ *siano così piccoli da verificare la disuguaglianza di Kraft*. La proposizione precedente, invece, assicura che non abbiamo costi aggiuntivi, relativamente alle lunghezze delle parole, se vogliamo passare da un codice decifrabile ad un codice istantaneo.

Sia $\mathcal{M} = \{m_1, m_2, \ldots, m_r\}$ un insieme finito con r elementi. Una funzione iniettiva $f : \mathcal{M} \to F^*$ si chiama *funzione di codifica* di $\mathcal{M}$ sull'alfabeto F. L'immagine $C = f(\mathcal{M})$ della funzione f, cioè

$$C = \{\boldsymbol{a} \in F^* \text{ tale che } f(m_i) = \boldsymbol{a}, m_i \in \mathcal{M}\},$$

è un codice su F (*codice di f)* e la coppia (C, f) si dice *schema di codifica di $\mathcal{M}$ su C,* o *codifica* di $\mathcal{M}$ su C.
Assegnata la codifica (C, f) di $\mathcal{M}$, la funzione f, considerata come funzione tra $\mathcal{M}$ e C è biunivoca e, quindi, ogni parola di C è immagine di un unico elemento di $\mathcal{M}$. La funzione

$$f^{-1} : C \to \mathcal{M}$$

si chiama *funzione di decodifica,* o *decodifica* di C.

ESEMPIO 26

Sia $\mathcal{M} = Z_2^4$ l'insieme delle quaterne ordinate di elementi di $Z_2 = \{0, 1\}$. L'applicazione

$$f : (a, b, c, d) \in \mathcal{M} \rightarrow (a + b + d, a + c + d, a, b + c + d, b, c, d) \in Z_2^7$$

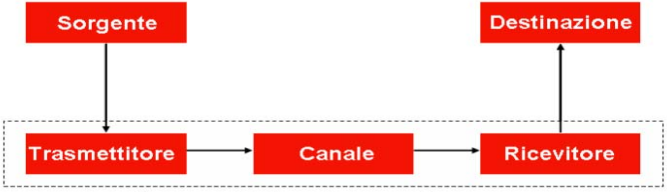
è una funzione di codifica di $\mathcal{M}$ su Z_2 il cui codominio è il $(7, 16)-$codice binario di Hamming.

ESEMPIO 27

Sia $\mathcal{M} = Z_3^2$ l'insieme delle coppie ordinate di elementi di $Z_3 = \{0, 1, 2\}$. L'applicazione

$$f : (a, b) \in \mathcal{M} \rightarrow (a, b, a, a + b, -a - b) \in Z_3^4$$

è una funzione di codifica di $\mathcal{M}$ su Z_3 il cui codominio è il $(4, 9)-$codice ternario di Hamming.


Sorgente
Destinazione
Trasmettitore
Canale
Ricevitore
Apparecchiatura di comunicazione

3. Sorgenti di informazione, compressione di dati e teorema di Shannon per la codifica delle sorgenti

indice

Sorgenti di informazione

Una *sorgente di informazione* (finita) $\mathcal{S}$, o più semplicemente *sorgente*, può pensarsi come un sistema fisico in grado di emettere con regolarità dei segnali o simboli corrispondenti alle lettere di un alfabeto finito $A = \{a_1, a_2, \ldots, a_q\}$ con q lettere. Questo significa che esiste un numero reale $R > 0$, detto *tasso di emissione*, tale che in ogni intervallo temporale di ampiezza T vengono emessi RT segnali. Per il momento non è restrittivo supporre $R = 1$: un segnale per ogni unità di tempo.
Denoteremo con

$$(X_n) = X_0 X_1 \cdots X_n \cdots \tag{3}$$

la successione dei simboli emessi dalla sorgente $\mathcal{S}$ a partire da un istante iniziale $t = 0$, ove X_i denota il simbolo emesso nell'istante $t = i$.
Denoteremo, inoltre, con

$$P(X_i = a_j) \tag{4}$$

la probabilità che l'$i-$esimo elemento X_i della successione (3) sia uguale alla lettera $a_j \in A$.

Sorgenti senza memoria

DEFINIZIONE 28

La sorgente $\mathcal{S}$ si dice *senza memoria* se, per ogni i, j, la probabilità (4) dipende solo da j; cioè se sull'alfabeto A è definita una probabilità

$$p(a_j) = p_j, \text{ tale che} \tag{5}$$

$$P(X_i = a_j) = p_j \text{ , per ogni } i, j. \tag{6}$$

Se $\mathcal{S}$ è una sorgente senza memoria, la successione

$$\boldsymbol{p} = (p_1, p_2, \ldots, p_q)$$

si chiama *distribuzione di probabilità* di $\mathcal{S}$.

OSSERVAZIONE 29

Sostanzialmente la proprietà (6) dice che, per una sorgente senza memoria, il valore di X_i nella (3) non dipende nè dall'istante $t = i$ nè dai simboli emessi prima e dopo X_i; esso dipende soltanto dalla funzione di probabilità (5).

LANCIO DI UN DADO

Un esempio classico di sorgente di informazione senza memoria è quello corrispondente al lancio di un dado, le cui facce sono identificate dagli interi da 1 a 6. Qui per l'alfabeto A si ha $A = \{1, 2, 3, 4, 5, 6\}$ e, se il dado non è truccato, gli elementi di A sono equiprobabili, cioè

$$p_1 = p_2 = p_3 = p_4 = p_5 = p_6 = \frac{1}{6}\,.$$

LANCIO DI DUE DADI

Un altro esempio di sorgente di informazione senza memoria è quello corrispondente al lancio di due dadi. Qui l'alfabeto A è l'insieme degli interi che si ottengono sommando una faccia del primo dado ad una del secondo, cioè $A = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ e, se i dadi non sono truccati, la distribuzione di probabilità della sorgente è

$$\left(\frac{1}{36}, \frac{1}{18}, \frac{1}{12}, \frac{1}{9}, \frac{5}{36}, \frac{1}{6}, \frac{5}{36}, \frac{1}{9}, \frac{1}{12}, \frac{1}{18}, \frac{1}{36}\right).$$

OSSERVAZIONE 30

Per lo studio teorico di una sorgente di informazione senza memoria $\mathcal{S}$ è sufficiente conoscere l'alfabeto A e la funzione di probabilità (5). È, quindi, inessenziale qualsiasi riferimento ai dispositivi che permettono al sistema fisico $\mathcal{S}$ l'emissione di lettere di A. Ciò suggerisce di studiare il modello matematico descritto formalmente nella definizione che segue.

DEFINIZIONE 31

Una sorgente di informazione senza memoria ($q-$aria) è una coppia $\mathcal{S} = (A, p)$, ove A è un alfabeto finito con q lettere (alfabeto sorgente) e p una funzione di probabilità su A (distribuzione di probabilità).

Nel seguito prenderemo in considerazione soltanto sorgenti di informazione senza memoria e ne riterremo sempre fissata una

$$\mathcal{S} = (A, p),$$

con

$$A = \{a_1, a_2, \ldots, a_q\};$$

porremo, inoltre,

$$p(a_i) = p_i,$$

per ogni $i = 1, 2, \ldots, q$.

Assegnato l'alfabeto $A = \{a_1, a_2, a_3, a_4\}$, sia p la funzione di probabilità su A definita da

$$p(a_1) = p(a_2) = \frac{2}{17},\ p(a_3) = \frac{9}{17},\ p(a_4) = \frac{4}{17}\,.$$

Allora (A, p) è una sorgente di informazione senza memoria con distribuzione di probabilità

$$\left(\frac{2}{17}, \frac{2}{17}, \frac{9}{17}, \frac{4}{17}\right)$$

Assegnati l'alfabeto $A = \{a_1, a_2, \ldots, a_q\}$ e un numero reale ϵ positivo e minore di 1, sia p la funzione di probabilità su A definita da

$$p(a_1) = p(a_2) = \cdots = p(a_{q-1}) = \frac{\epsilon}{q-1},\ p(a_q) = 1 - \epsilon\,.$$

Allora (A, p) è una sorgente di informazione senza memoria con distribuzione di probabilità

$$\left(\frac{\epsilon}{q-q}, \frac{\epsilon}{q-1}, \ldots, \frac{\epsilon}{q-1}, 1-\epsilon\right)\,.$$

OSSERVAZIONE 32

La distribuzione di probabilità di una sorgente di informazione binaria $A = \{0, 1\}$ è necessariamente del tipo $(p, 1-p)$, con p numero reale positivo e minore di 1.

DEFINIZIONE 33

Siano assegnati una sorgente $\mathcal{S} = (A, p)$ ed un codice C su un alfabeto F. Una codifica (C, f) dell'alfabeto A, cioè una funzione biunivoca $f : A \to C$, prende il nome di *codifica della sorgente $\mathcal{S}$ su F*, o semplicemente *codifica della sorgente $\mathcal{S}$*, se F è noto dal contesto.

Per una codifica (C, f), il numero reale

$$\ell(C, p) = \sum_{i=1}^{q} |f(a_i)| p_i \,, \tag{7}$$

ove $|f(a_i)|$ denota la lunghezza della parola $f(a_i)$, si chiama *lunghezza media della codifica* e il codice C si dice *associato* a $\mathcal{S}$.

Se (C, f) è una codifica della sorgente $\mathcal{S} = (A, p)$, con $A = \{a_1, a_2, \ldots, a_q\}$, porremo $f(a_j) = \boldsymbol{a}_j$. Su C resta definita la seguente funzione di probabilità, che denoteremo ancora con p :

$$p(\boldsymbol{a}_j) = p(a_j) = p_j.$$

Inoltre, se C gode di una fissata proprietà, diremo che anche la codifica (C, f) gode della stessa proprietà. Per esempio, dire che (C, f) è una *codifica istantanea* significa che il codice C è istantaneo.

OSSERVAZIONE 34

L'efficienza di una codifica di sorgente viene valutata mediante la sua lunghezza media: *una codifica è più efficiente di un'altra se la lunghezza media della prima è minore di quella della seconda*.

ESEMPIO 35

Consideriamo la sorgente $\mathcal{S} = (A, p)$ con $A = \{a, b, c\}$, $p(a) = p(b) = \frac{1}{4}$ e $p(c) = \frac{1}{2}$.

(a) La funzione

$$a \to 0\,, \quad b \to 1\,, \quad c \to 01\,,$$

è una codifica binaria di $\mathcal{S}$ di lunghezza media $\frac{1}{4} + \frac{1}{4} + 2\frac{1}{2} = \frac{3}{2}$.

(b) La funzione

$$a \to 00\,, \quad b \to 11\,, \quad c \to 001\,,$$

è una codifica binaria di $\mathcal{S}$ di lunghezza media $2\frac{1}{4} + 2\frac{1}{4} + 3\frac{1}{2} = \frac{5}{2}$.

OSSERVAZIONE 36

La codifica (a) è da ritenersi più efficiente della (b).

Codici ottimi

PROBLEMA 37

Trovare codifiche istantanee con minima lunghezza media per una fissata sorgente $\mathcal{S} = (A, p)$.

DEFINIZIONE 38

Denotiamo con ℓ_{min} la minima lunghezza media delle codifiche istantanee di $\mathcal{S}$, cioè

$$\ell_{min} = min\{\ell(C, p) \ : \ (C, f) \text{ codifica istantanea di } \mathcal{S}\}.$$

Una codifica istantanea (C, f) si dice *ottima* se ha lunghezza media uguale a ℓ_{min}.
Un codice C si dice *ottimo* se è istantaneo ed esiste una codifica ottima (C, f) di $\mathcal{S}$.

OSSERVAZIONE 39

Una codifica di $\mathcal{S}$ mediante un codice ottimo non è altro che una procedura mediante la quale si codifica l'informazione emessa da $\mathcal{S}$ liberandola dalla ridondanza (*compressione dei dati*).

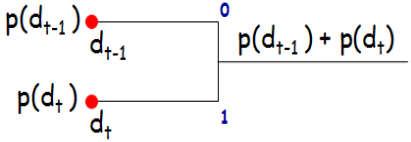
PROPOSIZIONE 40

Sia C un codice $q-$ario, su un alfabeto F, costituito dalle M parole $a_1, a_2, \ldots, a_M$ di rispettive lunghezze $\ell_1, \ell_2, \ldots, \ell_M$. Supponiamo $\ell_1 \leq \ell_2 \leq \cdots \leq \ell_M$ e che C sia un codice ottimo associato alla sorgente $\mathcal{S} = (A, p)$. Allora:

1. $p(a_i) > p(a_j) \Rightarrow \ell_i \leq \ell_j$;
2. *C contiene almeno due parole di lunghezza massima ℓ_M, cioè $\ell_{M-1} = \ell_M$;*
3. *nel codice C, per ogni parola a_s di lunghezza massima ℓ_M ne esiste un'altra a_t della stessa lunghezza che differisce da a_s solo sull'ultima componente.*

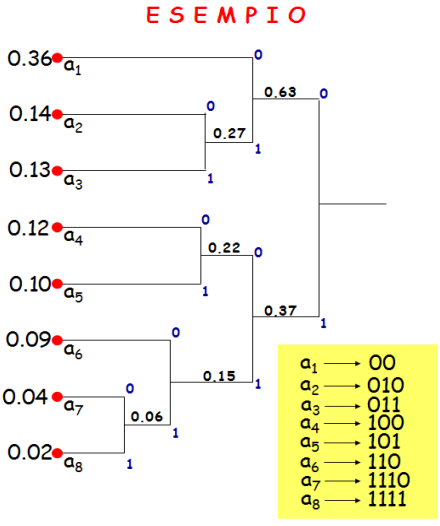
Codifica binaria di Huffman

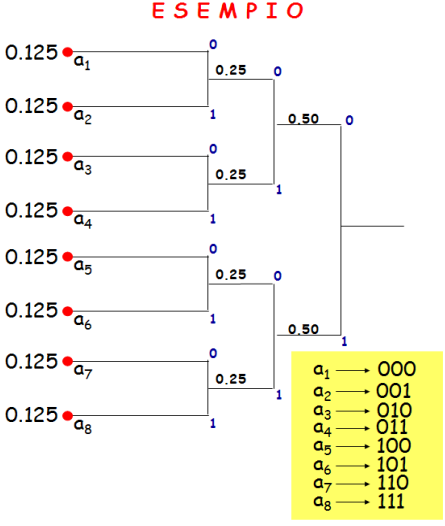
Assegnata la sorgente $\mathcal{S} = (A, p)$, $A = \{a_1, a_2, \ldots, a_q\}$, si può costruire una sua codifica binaria ottima usando il seguente *algoritmo di Huffman* (1952):
passo 1: Si ponga $t := q$ e si costruisca la successione $\{d_n\}$ delle lettere $a_1, a_2, \ldots, a_t$ ordinate secondo i valori non crescenti delle loro probabilità.
passo 2: Si identifichino gli ultimi due simboli d_{t-1} e d_t in un unico simbolo con probabilità $p(d_{t-1}) + p(d_t)$ e si associ 0 a d_{t-1} e 1 a d_t.



passo 3: Posto $t := t - 1$ si ripetano i passi 1 e 2 fino a $t = 1$, cioè finchè non rimane un unico simbolo.
codifica: Per ogni lettera $a_i \in A$, la parola di codice corrispondente si trova prendendo in ordine le lettere $0, 1$ che si trovano percorrendo a ritroso l'albero (= *grafo connesso senza circuiti*) generato con i passi 1, 2 e 3, dalla radice finale alla lettera fissata.

Codifica binaria di Huffman





Codifica di Huffman

Questa codifica, che prende il nome dal suo inventore David Huffman, è un algoritmo per la compressione di dati ancora molto usato, specialmente per la compressione di file di testo e di programmi (pkZIP, lha, gz, arj; in parte per JPEG, MPEG).

ESEMPIO 41

Consideriamo il testo

$$ANNATA,$$

che, codificato in ASCII esteso, è una parola binaria di lunghezza $6 \times 8 = 48$.
Per il nostro testo l'alfabeto sorgente è $\{A, N, T\}$ con probabilità delle lettere $p(A) = \frac{1}{2}$, $p(N) = \frac{1}{3}$ e $p(T) = \frac{1}{6}$.
Una codifica di Huffman dell'alfabeto è la seguente: $A = 0$, $N = 10$, $T = 11$.
Questa permette di codificare *ANNATA* con la parola binaria di lunghezza 9 :

$$010100110.$$

Abbiamo risparmiato 39 lettere su 48 rispetto alla codifica ASCII !

Sia F^+ l'insieme delle lettere dell'alfabeto F con probabilità diversa da zero e consideriamo la funzione

$$I : a_i \in F^+ \longrightarrow \log_2 \frac{1}{p_i} = -\log_2 p_i. \tag{8}$$

DEFINIZIONE 42

Per $p_i \neq 0$, il valore

$$I(a_i) = \log_2 \frac{1}{p_i} = -\log_2 p_i \tag{9}$$

di I sulla lettera a_i si chiama *informazione* associata ad a_i, o anche *quantità di informazione*, o *informazione*, di a_i. Poichè $I(a_i)$ dipende esclusivamente dalla probabilità $p(a_i) = p_i$, a volte porremo anche

$$I(p_i) := I(a_i).$$

Se il simbolo X_i emesso dalla sorgente $\mathcal{S}$ è uguale ad a_j con $p_j \neq 0$, tenendo presente che $P(X_i = a_j) = p_j$, definiamo l'*informazione* $I(X_i)$ associata ad X_i come $I(X_i) = I(a_j)$.

CONVENZIONE 43

Quando nel seguito parleremo di informazione di una lettera dell'alfabeto F, sottointenderemo che la probabilità di tale lettera sia positiva.

OSSERVAZIONE 44

L'informazione $I(a_i)$ di una lettera a_i di F è tanto più grande quanto più piccola è la sua probabilità p_i. Ciò in accordo con quanto ci aspettiamo dall'intuizione: l'informazione fornita dal verificarsi di un evento è tanto più grande quanto più piccola è la sua probabilità.

ESEMPIO 45

Nel lancio di un dado, le lettere sono equiprobabili e, quindi, hanno tutte la stessa informazione.
Nel lancio di due dadi, le lettere non hanno tutte la stessa informazione. Le lettere con massima informazione sono 2 e 12; quella con minima informazione è 7.

ESEMPIO 46

Per una sorgente $\mathcal{S}$ con alfabeto binario $F = \{0, 1\}$ e

$$p(0) = 1 - p\,,\ p(1) = p\,,$$

risulta

$$I(0) = -\log_2(1-p)\,,\ \ I(1) = -\log_2 p,$$

se è $p > 0$. Si osservi che i casi

$$p = 0 \text{ e } p = 1$$

corrispondono, rispettivamente, ad una sorgente che emette sempre la lettera 0 ($p(0) = 1\,,\ p(1) = 0$) ovvero la lettera 1 ($p(0) = 0\,,\ p(1) = 1$).
Si osservi ancora che quando le lettere $0, 1$ sono equiprobabili, cioè $p = \frac{1}{2}$, risulta

$$I(0) = I(1) = 1.$$

OSSERVAZIONE 47

Una sorgente con due lettere equiprobabili corrisponde agli esiti dei lanci di una moneta (non truccata).

DEFINIZIONE 48

L'informazione di una lettera di una sorgente binaria con alfabeto equiprobabile si chiama *bit* e si assume come unità di misura dell'informazione.

DEFINIZIONE 49

Si chiama *entropia* della sorgente $\mathcal{S}$, o *informazione totale*, e si denota con $H(\mathcal{S})$, il numero reale (media di $I(\mathcal{S})$ considerata come variabile aleatoria)

$$H(\mathcal{S}) = H(p_1, p_2, \ldots, p_q) := \sum_{i=1}^{q} p(a_i) I(a_i) \tag{10}$$

e, quindi,

$$H(\mathcal{S}) = \sum_{i=1}^{q} p_i \log_2 \frac{1}{p_i} = -\sum_{i=1}^{q} p_i \log_2 p_i. \tag{11}$$

OSSERVAZIONE 50

L'entropia di $\mathcal{S}$ misura la quantità d'informazione media fornita dalla sorgente $\mathcal{S}$ o, equivalentemente, la nostra incertezza su $\mathcal{S}$.

PROPOSIZIONE 51

Risulta

$$H(p_1, p_2, \ldots, p_q) \leq \log_2 q,$$

l'uguaglianza avendosi se, e solo se

$$p_1 = p_2 = \cdots = p_q = \frac{1}{q}.$$

ESEMPIO 52

Quando le q lettere $a_1, a_2, \ldots, a_q$ di una sorgente $\mathcal{S}$ sono equiprobabili, cioè

$$p_1 = p_2 = \cdots = p_q = \frac{1}{q},$$

l'entropia di $\mathcal{S}$ coincide con l'informazione associata ad una qualsiasi lettera a_i

$$H(\mathcal{S}) = \sum_{i=1}^{q} p_i \log_2 \frac{1}{p_i} = q\frac{1}{q}\log_2 q = \log_2 q = I(a_i).$$

Ne segue che quando

$$q = 2 \quad \text{e} \quad p_1 = p_2 = \frac{1}{2},$$

l'entropia di $\mathcal{S}$ è uguale ad 1 (cfr. esempio 46).

DEFINIZIONE 53

L'entropia di una sorgente con $q = 2$ e $p_1 = p_2 = \frac{1}{2}$, si chiama *bit* e si assume come unità di misura delle entropie.

OSSERVAZIONE 54

Se n è un intero positivo, una sorgente con entropia di n bit equivale all'informazione fornita da n risposte *SI* o *NO* a domande poste in modo che le risposte *SI* o *NO* siano equiprobabili.

Per una sorgente $\mathcal{S}$ con alfabeto binario $F = \{0, 1\}$ e $p(0) = 1 - p\,,\ p(1) = p\,$, l'entropia risulta

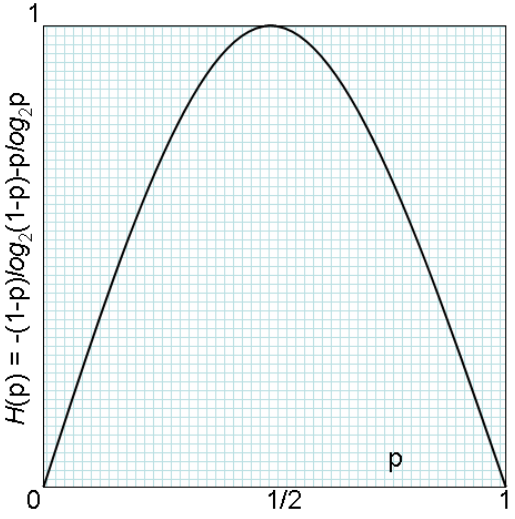
$$H(\mathcal{S}) = -(1-p)\log_2(1-p) - p\log_2 p.$$

Si osservi che risulta $H(\mathcal{S}) = 0$ se, e solo se, $p = 0$ oppure $p = 1$. In questi due casi non abbiamo alcuna informazione: essi corrispondono ad una sorgente che emette sempre la lettera 0 ($p(0) = 1\,,\ p(1) = 0$) ovvero la lettera 1 ($p(0) = 0\,,\ p(1) = 1$), rispettivamente.
Si osservi ancora che $H(\mathcal{S})$ è massima quando

$$p = \frac{1}{2},$$

cioè quando le elttere $0, 1$ sono equiprobabili. In questo caso non è mai possibile prevedere quale lettera sarà emessa dalla sorgente.

Entropia di una sorgente binaria



Sia $\mathcal{S} = (F, p)$ una sorgente di informazione senza memoria con entropia $H(\mathcal{S})$ e F' un alfabeto con t lettere. Allora, se (C, f) è una codifica dell'alfabeto F su F', risulta

$$\frac{H(\mathcal{S})}{\log_2 t} \leq \ell(C, p). \tag{12}$$

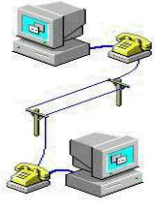
Inoltre, per ogni numero reale $\ell \geq H(\mathcal{S})/\log_2 t$, esiste almeno una codifica (C, f) di F la cui lunghezza media è uguale ad ℓ.

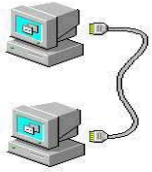
ESEMPIO 55

Se $\mathcal{S}$ è una sorgente senza memoria su un alfabeto con 2^n lettere equiprobabili, allora $H(S) = n$ e, in forza della (12), una sua codifica binaria non può avere tutte le parole di lunghezza minore di n :

$$2 + 2^2 + \cdots + 2^{n-1} < 2^n \ !$$

4. Canali di trasmissione





indice

Per *canale di trasmissione*, o *di comunicazione*, intendiamo un sistema fisico in grado di accettare in una *entrata* dei segnali o simboli corrispondenti alle lettere di un alfabeto

$$F = \{a_1, a_2, \cdots, a_q\} \text{ (alfabeto di input)}$$

e, in corrispondenza di ciascun segnale accettato, emettere in una *uscita* segnali corrispondenti alle lettere di un alfabeto

$$F' = \{b_1, b_2, \cdots, b_t\} \text{ (alfabeto di output)}.$$

Escludiamo la possibilità che all'immissione di una lettera in input non corrisponda l'emissione di una lettera in output.

CONVENZIONE 56

Per motivi di semplicità, supporremo sempre che gli alfabeti di input e di output coincidano.

DEFINIZIONE 57

Quando in un canale di trasmissione Σ si immettono successivamente le lettere $a_{i_1}, a_{i_2}, ..., a_{i_n}$ e in uscita si hanno nell'ordine le lettere $a_{j_1}, a_{j_2}, ..., a_{j_n}$ diremo che è stata trasmessa la parola

$$\boldsymbol{a}_i = (a_{i_1}, a_{i_2}, ..., a_{i_n})$$

e che è stata ricevuta la parola

$$\boldsymbol{a}_j = (a_{j_1}, a_{j_2}, ..., a_{j_n}).$$

In queste ipotesi, il numero di componenti omologhe distinte tra $\boldsymbol{a}_i$ e $\boldsymbol{a}_j$ prende il nome di *numero di errori* commesso nella trasmissione della parola $\boldsymbol{a}_i$.

ESEMPIO 58

Supponiamo di avere in input la parola $\boldsymbol{a} = 01111101$ e in output la parola $\boldsymbol{b} = 0101101000$. Tali parole hanno lettere differenti nella seconda, quinta e ottava posizione e, quindi, il numero di errori su $\boldsymbol{a}$ è 3.

Per ogni $a_i, a_j \in F$, denotiamo con

$$P(a_j \ ric \,|\, a_i \ inv) \quad \text{o con} \quad P(a_j \,|\, a_i)$$

la probabilità condizionata di ricevere nell'uscita del canale Σ la lettera a_j dopo che è stata immessa in entrata la lettera a_i e supponiamo che tale probabilità dipenda soltanto dalla coppia (a_i, a_j).
In queste ipotesi, il canale di trasmissione si dice *senza memoria* e, posto

$$p_{ij} := P(a_j \,|\, a_i), \tag{13}$$

la matrice $P := (p_{ij})$ si chiama *matrice di transizione del canale rispetto all'alfabeto* F. Quando l'alfabeto è chiaro dal contesto si parla semplicemente di *matrice di* Σ.

OSSERVAZIONE 59

P è una matrice stocastica, cioè la somma degli elementi su ogni riga di P è uguale ad 1 :

$$0 \leq p_{ij} \leq 1 \quad e \quad \sum_{j=1}^{q} p_{ij} = 1 \,.$$

OSSERVAZIONE 60

Per lo studio teorico di un canale senza memoria Σ è sufficiente conoscere l'alfabeto F e la matrice del canale P. Come per una sorgente d'informazione senza memoria, è inessenziale qualsiasi riferimento alla struttura hardware del sistema fisico adottato per la trasmissione dell'informazione.

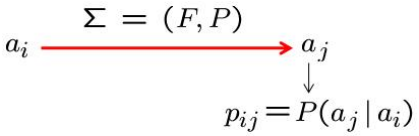
Questa osservazione suggerisce di dare la seguente definizione formale.

DEFINIZIONE 61

Un *canale senza memoria* è una coppia $\Sigma = (F, P)$, ove F è un alfabeto finito con q lettere e $P = (p_{ij})$ una matrice quadrata stocastica d'ordine q detta *matrice del canale* o *matrice delle probabilità di transizione*. Quando P non è la matrice identità, il canale si dice *rumoroso*.

OSSERVAZIONE 62

Assegnato un canale senza memoria $\Sigma = (F, P)$, un elemento p_{ij} della matrice P deve interpretarsi come la probabilità condizionata di ricevere nell'uscita del canale la lettera a_j dopo che è stata immessa in entrata la lettera a_i.



OSSERVAZIONE 63

Un canale senza memoria (F, P) per cui la matrice P è l'dentità, cioè $p_{ii} = 1$, per ogni indice i, si dice *perfetto*, o *senza rumore*. Un canale senza rumore è deterministico, nel senso che all'immissione di una lettera dell'alfabeto F corrisponde sempre l'emissione della stessa lettera.

Canali simmetrici

Un canale si dice *simmetrico* se la probabilità p che una lettera a_i in input sia trasformata in output in una lettera diversa a_j non dipende da a_i e a_j, ma è la stessa per tutte le coppie di lettere distinte.
Nella matrice P di un canale simmetrico risulta $p_{ij} = p$, per ogni coppia (i, j), con $i \neq j$, quindi:

$$P = \begin{bmatrix} 1-(m-1)p & p & \dots & p \\ p & 1-(m-1)p & \dots & p \\ \vdots & \vdots & \ddots & \vdots \\ p & p & \dots & 1-(m-1)p \end{bmatrix}$$

Il numero p si chiama *probabilità d'errore* del canale.
In particolare, si dicono *canali simmetrici binari* quelli che operano con un alfabeto binario, per esempio $\{0, 1\}$. La matrice di tali canali è data da

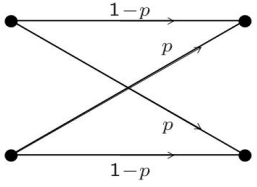
$$P = \begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix}.$$

Per un canale simmetrico binario con probabilità d'errore p si ha che:

(a) la probabilità che nella trasmissione di una parola di lunghezza n si verifichino k errori è

$$\binom{n}{k} p^k (1-p)^{n-k} ;$$

(b) il numero di errori atteso nella trasmissione di una parola di lunghezza n è np.



Canali di trasmissione senza memoria

Siano $\boldsymbol{a}_i = (a_{i_1}, a_{i_2}, ..., a_{i_n})$ e $\boldsymbol{a}_j = (a_{j_1}, a_{j_2}, ..., a_{j_n})$ due parole di lunghezza n su F e denotiamo con

$$P(\boldsymbol{a}_j \ ric \,|\, \boldsymbol{a}_i \ inv) \ \text{ o } \ P(\boldsymbol{a}_j \,|\, \boldsymbol{a}_i)$$

la probabilità condizionata di ricevere nell'uscita del canale Σ la parola $\boldsymbol{a}_j$ dopo che è stata immessa in entrata la parola $\boldsymbol{a}_i$ Risulta

$$P(\boldsymbol{a}_j \,|\, \boldsymbol{a}_i) = P(a_{j_1} \,|\, a_{i_1}) P(a_{j_2} \,|\, a_{i_2}) \cdots P(a_{j_n} \,|\, a_{i_n}) \ . \tag{14}$$

Ordiniamo linearmente l'insieme

$$F^n = \{\boldsymbol{a}_1, \boldsymbol{a}_2, ...\} \ ,$$

e poniamo

$$p_{ij}^{(n)} := P(\boldsymbol{a}_j \,|\, \boldsymbol{a}_i) \ .$$

DEFINIZIONE 64

la matrice stocastica

$$P^{(n)} := \left(p_{ij}^{(n)} \right) \tag{15}$$

prende il nome di *n-esima matrice del canale* Σ (rispetto all'alfabeto F).

OSSERVAZIONE 65

$P^{(n)}$ può riguardarsi come la matrice di Σ rispetto ad F^n, considerato come alfabeto.

ESEMPIO 66

Sia Σ un canale binario simmetrico con probabilità d'errore p. Allora, se $\{(0,0),(0,1),(1,0),(1,1)\}$ è l'insieme linearmente ordinato delle parole binarie di lunghezza 2, la seconda matrice di Σ è data da

$$P^{(2)} = \begin{bmatrix} (1-p)^2 & p(1-p) & p(1-p) & p^2 \\ p(1-p) & (1-p)^2 & p^2 & p(1-p) \\ p(1-p) & p^2 & (1-p)^2 & p(1-p) \\ p^2 & p(1-p) & p(1-p) & (1-p)^2 \end{bmatrix} = \begin{bmatrix} (1-p)P & pP \\ pP & (1-p)P \end{bmatrix} = P \otimes P.$$

ESERCIZIO 67

Sia $P^{(n)}$ la $n-$esima matrice di un canale simmetrico binario. Provare che ogni riga (risp. colonna) di $P^{(n)}$ è una permutazione della prima.

5. Entropia e capacità di un canale senza memoria

indice

Assegnato un canale senza memoria

$$\Sigma = (F, P = (p_{ij})), \text{ con } F = \{a_1, a_2, \ldots, a_q\},$$

oltre alle probabilità di transizione

$$(p_{ij}) = P(a_j|a_i) = P(a_j \ ric \,|\, a_i \ inv),$$

sono di interesse anche le seguenti probabilità:

- $P(a_i \ inv)$ = probabilità che entri nel canale la lettera a_i.
- $P(a_i \ ric)$ = probabilità che esca dal canale la lettera a_i.
- $P(a_i, a_j)$ = probabilità congiunta che entri nel canale la lettera a_i e esca a_j.
- $P(a_i \ inv \,|\, a_j \ ric)$ = probabilità condizionata che sia entrata nel canale la lettera a_i sapendo che è uscita la lettera a_j.

Se abbiamo un canale senza memoria $\Sigma = (F, P = (p_{ij}))$, con $F = \{a_1, a_2, \ldots, a_q\}$ possiamo pensare che Σ accetti in entrata le lettere di F dopo che siano state emesse da una sorgente di informazione. Se supponiamo che tale sorgente sia una sorgente $\mathcal{S} = (F, p)$ senza memoria, abbiamo

$$p_i = P(a_i \ inv) \ , \quad P(a_j \ ric) = \sum_{i=1}^{q} P(a_j|a_i)P(a_i \ inv) = \sum_{i=1}^{q} p_i p_{ij}$$

OSSERVAZIONE 68

Quando $\Sigma = (F, P = (p_{ij}))$ accetta in entrata le lettere di una sorgente senza memoria $\mathcal{S} = (F, p)$ e poniamo $t(a_i) = P(a_i \ ric)$, l'uscita può riguardarsi come una sorgente senza memoria $\mathcal{T} = (F, t)$.

$$\mathcal{S} = (F, p) \xrightarrow{\Sigma = (F, P)} \mathcal{T} = (F, t)$$

DEFINIZIONE 69

Siano a_j un fissato elemento dell'alfabeto $F = \{a_1, a_2, \ldots, a_q\}$. Il numero reale

$$-\sum_{i=1}^{q} P(a_i \ inv \mid a_j \ ric) \log_2 P(a_i \ inv \mid a_j \ ric) \tag{16}$$

si denota con $H_j(\mathcal{S})$, o con $H(\mathcal{S} \mid a_j)$, e si chiama *entropia condizionata di $\mathcal{S}$ alla ricezione di a_j*.

DEFINIZIONE 70

Il numero reale

$$H(\mathcal{S} \mid \mathcal{T}) = \sum_{i=1}^{q} t_i H_i(\mathcal{S}) \tag{17}$$

si chiama *entropia condizionata di $\mathcal{S}$ dato $\mathcal{T}$ o equivocità di $\mathcal{S}$ sul canale Σ*.

OSSERVAZIONE 71

L'entropia condizionata di $\mathcal{S}$ dato $\mathcal{T}$

$$H(\mathcal{S} \mid \mathcal{T}) = \sum_{i=1}^{q} t_i H_i(\mathcal{S})$$

misura l'informazione perduta in media su un simbolo trasmesso dopo l'osservazione del simbolo ricevuto. Ne segue che, sottraendo tale quantità all'entropia di $\mathcal{S}$, si ottiene la quantità di informazione fornita da $\mathcal{T}$ su $\mathcal{S}$.

DEFINIZIONE 72

Il numero reale

$$I(\mathcal{S}, \mathcal{T}) = H(\mathcal{S}) - H(\mathcal{S} \mid \mathcal{T}) \tag{18}$$

si chiama *mutua informazione tra $\mathcal{S}$ e $\mathcal{T}$*, o *flusso medio di informazione*.

PROPOSIZIONE 73

$$I(\mathcal{S}, \mathcal{T}) = I(\mathcal{T}, \mathcal{S}).$$

OSSERVAZIONE 74

Si può dimostrare che la mutua informazione $I(\mathcal{S};\mathcal{T})$ è funzione soltanto della distribuzione di probabilità $(p_1, p_2, \ldots, p_q)$ di $\mathcal{S}$ e della matrice P del canale Σ.

PROPOSIZIONE 75

Sia **S** *l'insieme delle sorgenti senza memoria. Allora l'insieme*

$$\{I(\mathcal{S};\mathcal{T}) \ : \ \mathcal{S} \in \mathbf{S}\} \tag{19}$$

ammette il massimo (si osservi che tale massimo dipende soltanto da Σ).

DEFINIZIONE 76

Il massimo C_Σ dell'insieme (19) si chiama di *capacità* del canale di trasmissione senza memoria Σ. In altre parole, C_Σ è il massimo flusso di informazione al variare della distribuzione delle probabilità della sorgente $\mathcal{S}$.

6. Sistemi di comunicazione discreti e teorema di Shannon per la codifica di canale

indice

PROBLEMA 77

Assegnati una sorgente di informazione $\mathcal{S}$, e un canale di trasmissione soggetto a disturbi (rumore), vogliamo studiare il seguente problema: *partendo da una codifica compatta C dell'alfabeto sorgente, trovare una codifica di C che permetta di trasmettere nel modo più efficiente possibile attraverso* Σ.

Trasmissioni con rumore

- Supponiamo che $\mathcal{S}$ sia binaria con lettere equiprobabili e che abbia tasso di emissione $R = \frac{1}{3}$, cioè emetta un bit ogni 3 secondi.
- Supponiamo anche che Σ abbia la capacità di trasmettere un bit al secondo con probabilità d'errore $p < \frac{1}{2}$ in ricezione.
- È chiaro che, in queste ipotesi, qualunqe sia la modalità di trasmissione, la velocità con cui si riconoscono in ricezione i bit emessi da $\mathcal{S}$ non può essere superiore a un bit ogni 3 secondi.

La trasmissione più naturale è quella di inviare attraverso Σ un bit emesso da $\mathcal{S}$ ogni tre secondi:

$$\mathcal{S} \longrightarrow \cdots - - x_3 - - x_2 - - x_1 \xrightarrow{\Sigma} \cdots - - y_3 - - y_2 - - y_1$$

In questo modo la probabilità P_Σ che un bit emesso da $\mathcal{S}$ venga ricevuto in errore è $P_\Sigma = p$, cioè la probabilità di ricevere un bit uguale ad uno trasmesso è $1 - p$.

Se vogliamo migliorare la trasmissione,
dobbiamo trovare una strategia
che permetta di diminuire la probabilità P_Σ!

Trasmettiamo ogni bit emesso da $\mathcal{S}$ ripetendolo due volte, cioè codifichiamo 0 con 00 e 1 con 11. La velocità con cui si riconoscono in ricezione i bit emessi da $\mathcal{S}$ è ancora di un bit ogni 3 secondi:

$$\mathcal{S} \longrightarrow \cdots - -x_3 - -x_2 - -x_1$$

$$\textit{codifica di sorgente} \longrightarrow \cdots - x_3x_3 - x_2x_2 - x_1x_1$$

$$\Sigma \longrightarrow \cdots - y_{32}y_{31} - y_{22}y_{21} - y_{12}y_{11}$$

In queste ipotesi, non abbiamo alcun criterio per decodificare, in arrivo, le parole 10 e 01 : possiamo solo decodificarle in modo random con 00 o 11. Allora, per la probabilità P'_Σ che un bit emesso da $\mathcal{S}$ venga ricevuto (decodificato) in errore, abbiamo:

$$P'_\Sigma = \frac{1}{2}(\textit{ probabilità di 1 errore di canale su una parola di 2 bit})$$

$$+ \textit{ probabilità di 2 errori di canale su una parola di 2 bit}$$

$$= p(1-p) + p^2 = p = P_\Sigma.$$

In questo modo, dunque, non è possibile diminuire P_Σ.
Quello che potremmo fare è rinunciare a decodificare 10 e 01. Questo significa che se si riceve una di queste parole, bisogna chiedere una nuova trasmissione.

Possiamo fare di più!

Trasmettiamo ogni bit emesso da $\mathcal{S}$ ripetendolo tre volte, cioè codifichiamo 0 con 000 e 1 con 111. La velocità con cui si riconoscono in ricezione i bit emessi da $\mathcal{S}$ è ancora di un bit ogni 3 secondi:

$$\mathcal{S} \longrightarrow \cdots - - x_3 - - x_2 - - x_1$$

$$\textit{codifica di sorgente} \longrightarrow \cdots x_3 x_3 x_3 x_2 x_2 x_2 x_1 x_1 x_1$$

$$\Sigma \longrightarrow \cdots y_{32} y_{32} y_{31} y_{23} y_{22} y_{21} y_{13} y_{12} y_{11}$$

Decodifichiamo una parola di lunghezza 3 col bit che compare più volte come lettera della parola.
In queste ipotesi, per la probabilità P''_Σ che un bit emesso da $\mathcal{S}$ venga ricevuto (decodificato) in errore, abbiamo:

$$P''_\Sigma = \textit{ probabilità di 2 errori di canale su una parola di 3 bit}$$

$$+ \textit{ probabilità di 3 errori di canale su una parola di 3 bit}$$

$$= 3p^2(1-p) + p^3 = 3p^2 - 2p^3 < p = P_\Sigma \quad (\text{ricordiamo che è } p < \frac{1}{2}).$$

Un buon risultato: abbiamo diminuito P_Σ lasciando inalterati i tempi di trasmissione.

Possiamo fare di più ?

A questo punto è chiaro che, se codifichiamo i bit della sorgente con parole di lunghezza dispari maggiore di tre possiamo diminuire ancora P_Σ ma, questa volta, a scapito dei tempi di trasmissione e della sincronizzazione tra emissione della sorgente e trasmissione nel canale (una parola di 5 bit che rappresenti un bit emesso dalla sorgente non può essere trasmessa in 3 secondi!).

Si può, dunque, migliorare l'affidabilità di un sistema di comunicazione usando opportuni codici per la codifica dell'alfabeto sorgente. I possibili miglioramenti, però, sono condizionati dalle caratteristiche del sistema stesso.

Il teorema di Shannon, che enunceremo nel seguito, renderà matematicamente preciso il senso di queste nostre conclusioni euristiche.

Per *sistema di comunicazione discreto* intendiamo un sistema (**E**,Σ,**R**) composto da

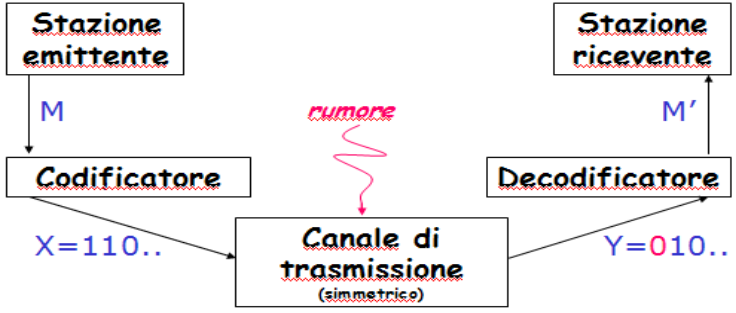
- una *stazione emittente* **E**, che possiamo identificare con una sorgente d'informazione finita $\mathcal{S} = (F, p)$;
- un *canale di trasmissione senza memoria* $\Sigma = (F, P)$ con *alfabeto* F e *matrice* P;
- una *stazione ricevente* **R ;**

di modo che

- la stazione **E**, mediante il canale Σ, invia ad **R** un messaggio (parola) M scelto in un prefissato codice (istantaneo) $\mathcal{M}$ (*insieme dei messaggi*);
- il messaggio M di $\mathcal{M}$, per essere accettato da Σ, viene *codificato* con una parola $\mathbf{x} = \gamma(M)$ di un codice C mediante una *funzione di codifica* (*codifica di canale*) γ che è una funzione biunivoca tra $\mathcal{M}$ e C;
- la parola **x** viene inviata attraverso il canale Σ e, in corrispondenza dell'entrata **x**, si trova in uscita una parola **y** che, a causa del rumore del canale, può essere diversa da **x**.
- se $\mathbf{y} \in C$, **y** si decodifica nel messaggio *M'* corrispondente; se $\mathbf{y} \notin C$, **y** si decodifica in un messaggio *M'* ottenuto con un opportuno algoritmo che massimizza la probabilità che sia *M=M'*; il messaggio *M'* così ottenuto è consegnato alla stazione ricevente **R.**

$$\mathbf{E} \longrightarrow M \overset{codifica}{\longrightarrow} \mathbf{x} = \gamma(M) \overset{\Sigma}{\longrightarrow} \mathbf{y} \overset{decodifica}{\longrightarrow} M' \rightarrow \mathbf{R}$$

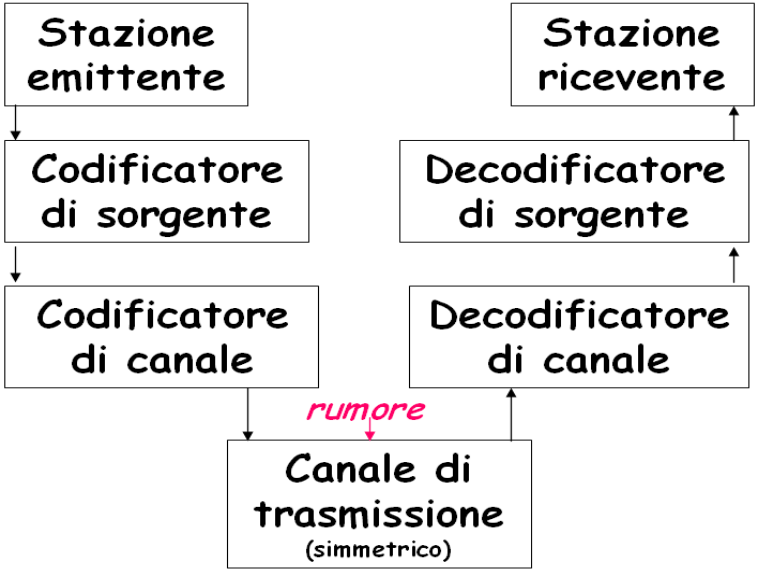
SISTEMA DI COMUNICAZIONE



PROBLEMA

Fare in modo che sia M=M'

SISTEMA DI COMUNICAZIONE



Probabilità di errore

Sia assegnato un sistema di comunicazione discreto (**E**,Σ,**R**) e sia C il codice usato per la codifica di canale.

DEFINIZIONE 78

Per ogni parola $\mathbf{a} \in C$, si chiama *probabilità di errore di* **a** e si denota con $p_e(\mathbf{a})$, la probabilità che all'immissione della parola **a** nel canale Σ corrisponda in uscita una parola diversa da **a**.
Il numero reale (media delle probabilità d'errore delle parole di C)

$$e(C) = \frac{1}{|C|} \sum_{a \in C} p_e(\mathbf{a})$$

si chiama *probabilità di errore* di C.
Il numero reale

$$\hat{e}(C) = \max\{p_e(\mathbf{a}) \ : \ \mathbf{a} \in C\}$$

si chiama *massima probabilità di errore di* C.

Teorema di Shannon

The noisy coding theorem

Sia assegnato un sistema di comunicazione con canale di trasmissione senza memoria $\Sigma = (F, P)$ di capacità C_Σ e con sorgente di informazione senza memoria $\mathcal{S} = (F, p)$ di entropia $H = H(\mathcal{S})$.
Allora, per ogni numero reale $\epsilon > 0$, si ha:

1. *per $H \leq C_\Sigma$, esiste un codice C ed una sua codifica di canale tale che*

$$\hat{e}(C) < \epsilon \ ;$$

2. *per $H > C_\Sigma$, esiste un codice C ed una sua codifica di canale tale che*

$$H - C_\Sigma \leq \hat{e}(C) < H - C_\Sigma + \epsilon \ ;$$

inoltre, non esiste alcun codice C con codifica di canale tale che

$$\hat{e}(C) < H - C_\Sigma .$$

Se un canale ha capacità C_Σ ed una sorgente ha entropia (tasso di informazione) $H \leq C_\Sigma$, allora esiste un sistema di codifica tale che l'uscita della sorgente può essere trasmessa sul canale con frequenza di errore piccola a piacere.
Viceversa se è $H > C_\Sigma$, allora non è possibile trasmettere l'informazione senza errori.

OSSERVAZIONE 79

La dimostrazione del teorema di Shannon non è di tipo costruttivo. Questo significa che non si conoscono metodi che permettano di costruire i codici di cui alla tesi del teorema stesso.

PROBLEMA 80

Assegnato un sistema di comunicazione, costruire codici C con codifiche di canale tali che le rispettive massime probabilità di errore $\hat{e}(C)$ siano le più piccole possibili.

PROPOSIZIONE 81

La capacità C_p di un canale simmetrico binario con probabilità d'errore p dipende solo da p e risulta

$$C_p = 1 + p \log_2 p + (1 - p) \log_2 (1 - p).$$

Il precedente teorema di Shannon, nel caso binario e simmetrico, può enunciarsi nel seguente modo.

TEOREMA 82

Sia assegnato un sistema di comunicazione con canale di trasmissione simmetrico binario con probabilità p e con sorgente d'informazione binaria. Allora, per ogni numero reale $\epsilon > 0$ e per ogni numero reale positivo $K < C_p$, esiste un codice C con tasso di informazione non inferiore ad K tale che $\hat{e}(C) < \epsilon$.

7. Decodifica e sistemi di comunicazione affidabili

indice

Decodifica

Sia $C = \{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_M\}$ un $(n, M)-$codice sull'alfabeto F.

DEFINIZIONE 83

Ua funzione

$$\pi \ : \ \mathbf{a} \in F^n \ \rightarrow \ \pi(\mathbf{a}) \in C$$

si chiama *decodifica di C*.

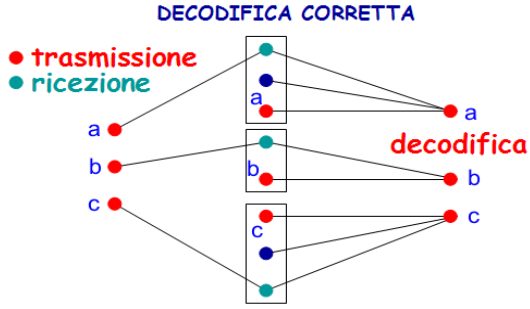
Una decodifica π di C individua la partizione (il *nucleo di* π)

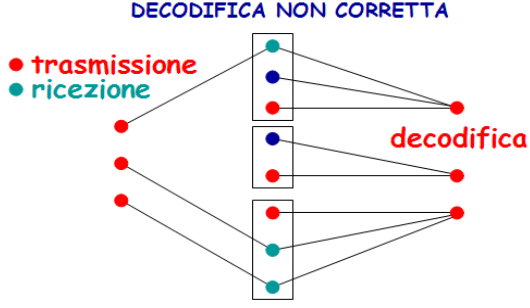
$$\Pi = \{B_a = \pi^{-1}(\mathbf{a}) \ : \ \mathbf{a} \in C\}$$

dell'insieme F^n delle parole su F di lunghezza n.

OSSERVAZIONE 84

Se le parole di C si trasmettono attraverso un canale senza memoria $\Sigma = (F, P)$, la decodifica π di C restituisce correttamente le parole inviate se, e solo se, ad ogni parola $\mathbf{x} \in C$ in entrata corrisponde in uscita una parola di B_x e $\mathbf{x} \in B_x$.


DECODIFICA CORRETTA
trasmissione
ricezione
a
b
c
a
b
c
decodifica
a
b
c


DECODIFICA NON CORRETTA
trasmissione
ricezione
decodifica

Ricevuta una parola $\mathbf{y}$, si consideri l'insieme I_y delle parole $\mathbf{x} \in C$ per cui $P(\mathbf{x}\ inv \,|\, \mathbf{y}\ ric)$ è il massimo dell'insieme

$$\{P(\mathbf{a}\ inv \,|\, \mathbf{y}\ ric) \ \text{ con } \ \mathbf{a} \in C\}\,.$$

1. Se I_y contiene una sola parola $\mathbf{x}$, allora $\mathbf{y}$ si decodifica con $\mathbf{x}$.
2. Nel caso contrario si richiede una nuova trasmissione o si decodifica $\mathbf{y}$ con una parola scelta in modo casuale in I_y.

OSSERVAZIONE 85

In forza del teorema di Bays, abbiamo

$$P(\mathbf{x}\ inv \,|\, \mathbf{y}\ ric) = \frac{P(\mathbf{y}\ ric \,|\, \mathbf{x}\ inv)P(\mathbf{x})}{\sum_{a\in C} P(\mathbf{y}\ ric \,|\, \mathbf{a}\ inv)P(\mathbf{a})}\,. \tag{20}$$

Ne segue che, per usare questa decodifica, oltre alla matrice di transizione delle probabilità del canale, dobbiamo conoscere anche le probabilità di ingresso delle parole del codice.

Ricevuta una parola $\mathbf{y}$, si consideri l'insieme M_y delle parole $\mathbf{x} \in C$ per cui $P(\mathbf{y}\ ric \,|\, \mathbf{x}\ inv)$ è il massimo dell'insieme

$$\{P(\mathbf{y}\ ric \,|\, \mathbf{a}\ inv) \ \text{ con } \ \mathbf{a} \in C\}.$$

1. Se M_y contiene una sola parola $\mathbf{x}$, allor $\mathbf{y}$ si decodifica con $\mathbf{x}$.
2. Nel caso contrario si richiede una nuova trasmissione o si decodifica $\mathbf{y}$ con una parola scelta in modo casuale in M_y.

OSSERVAZIONE 86

Per questa decodifica non è necessario conoscere le probabilità di ingresso delle parole del codice: basta soltanto la matrice di transizione delle probabilità del canale.

OSSERVAZIONE 87

Quando le parole di C hanno tutte la stessa probabilità di entrata ($p(\mathbf{x}) = \frac{1}{q}$, per ogni $\mathbf{x} \in C$), allora, in forza della (20), $P(\mathbf{x}\ inv \,|\, \mathbf{y}\ ric)$ è il massimo di I_y se e solo se $P(\mathbf{y}\ ric \,|\, \mathbf{x}\ inv)$ è il massimo di M_y. Ne segue che in questo caso le due decodifiche esposte restituiscono lo stesso risultato.

CONVENZIONE 88

Se $\mathbf{x} \in C$ entra nel canale di trasmissione, denotiamo con $\mathbf{y}$ la parola ricevuta, con $\mathbf{z} = \pi(\mathbf{y})$ la decodifica di $\mathbf{y}$ e supponiamo $P(\mathbf{y} \mid \mathbf{z}) \neq 0$.

DEFINIZIONE 89

Un sistema di comunicazione si dice *affidabile* se usa un codice C e una sua decodifica π tale che, per ogni $\mathbf{x} \in C$,
(1) $\mathbf{y} \in C \Leftrightarrow \mathbf{y} = \mathbf{x}$;
(2) deve aversi $\mathbf{z} = \mathbf{x}$, cioè $\mathbf{x}$ deve potersi riconoscere a partire da $\mathbf{y}$.

ESEMPIO 90

Le condizioni (1) e (2) di affidabilità del sistema sono evidentemente soddisfatte se valgono le seguenti proprietà:
(3) $P(\mathbf{a} \mid \mathbf{a}) \neq 0$, per ogni parola $\mathbf{a} \in C$;
(4) $P(\mathbf{b} \mid \mathbf{a}) = 0$ per ogni $\mathbf{a}, \mathbf{b}$ parole distinte di C;
(5) se $\mathbf{a} \in C$ e $P(\mathbf{c} \mid \mathbf{a}) \neq 0$, allora $P(\mathbf{c} \mid \mathbf{b}) = 0$ per ogni parola $\mathbf{b}$ di C diversa da $\mathbf{a}$.

Nelle ipotesi di affidabilità dell'Esempio 90 risulta:
(3) $P(\mathbf{a} \mid \mathbf{a}) \neq 0$, per ogni parola $\mathbf{a} \in C$;
(4) $P(\mathbf{b} \mid \mathbf{a}) = 0$ per ogni $\mathbf{a}, \mathbf{b}$ parole distinte di C;
(5) se $\mathbf{a} \in C$ e $P(\mathbf{c} \mid \mathbf{a}) \neq 0$, allora $P(\mathbf{c} \mid \mathbf{b}) = 0$ per ogni parola $\mathbf{b}$ di C diversa da $\mathbf{a}$; cioè gli insiemi

$$B_a = \{\mathbf{c} \in F^n \quad : \quad P(\mathbf{c} \mid \mathbf{a}) \neq 0\} ,$$

al variare di $\mathbf{a} \in C$, sono a due a due disgiunti.

È, quindi, naturale il seguente

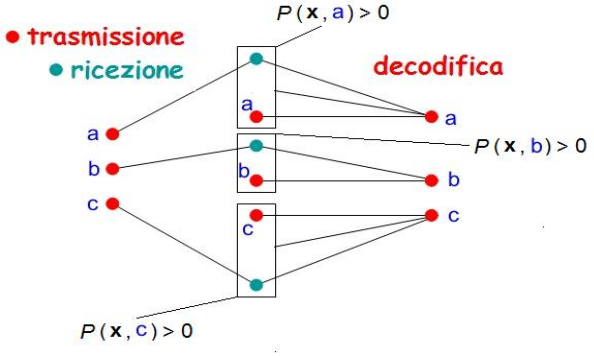
SCHEMA DI DECODIFICA 91

Se si riceve $\mathbf{y} \in B_x$, con $\mathbf{x} \in C$, si decodifica $\mathbf{y}$ con $\mathbf{x}$.

Con questo schema si decodifica senza commettere errori.

SCHEMA DI DECODIFICA 92

Nelle ipotesi di affidabilità dell'Esempio 90:
Se si riceve $\mathbf{y} \in B_x$, con $\mathbf{x} \in C$, si decodifica $\mathbf{y}$ con $\mathbf{x}$.



Per un sistema di comunicazione affidabile, la decodifica appena esposta è sia una decodifica *dell'osservatore ideale* che *di massima verosimiglianza.* Infatti, se si riceve una parola $\mathbf{y}$, esiste una sola parola $\mathbf{x} \in C$ tale che $\mathbf{y} \in B_x$ e quindi si ha

$$\{P(\mathbf{a}\ inv \,|\, \mathbf{y}\ ric) \neq 0 \ \text{ con } \ \mathbf{a} \in C\} = \{P(\mathbf{x}\ inv \,|\, \mathbf{y}\ ric)\}$$

e

$$\{P(\mathbf{y}\ ric \,|\, \mathbf{a}\ inv) \neq 0 \ \text{ con } \ \mathbf{a} \in C\} = \{P(\mathbf{y}\ ric \,|\, \mathbf{x}\ inv)\}\,.$$

È, dunque, importante
costruire codici che verifichino le proprietà (3), (4), (5)!

Conclusioni

Il problema fondamentale della comunicazione è quello di riprodurre in un punto, esattamente o approssimativamente, un messaggio scelto in un altro punto (C.Shannon).
Abbiamo visto che, anche in presenza di rumore, è sempre possibile codificare e trasmettere informazione in modo che, compatibilmente con la capacità del canale, gli errori si possano ridurre al minimo o addirittura eliminare.
I risultati che abbiamo illustrato, però, garantiscono l'esistenza ma non forniscono metodi per la costruzione di codici che realizzino un tale tipo di comunicazione.

La *teoria dei codici* studia le modalità per realizzare codifiche e decodifiche dell'informazione in modo da minimizzare la frequenza degli errori e, al contempo, consentire di sfruttare i canali di comunicazione al massimo delle loro capacità.

La *teoria dei codici lineari*, introdotta da R.Hamming, è un'importante parte della teoria dei codici particolarmente adatta ai problemi di correzione degli errori.

GENERALITÀ SUI CODICI

1. Distanza di Hamming

indice

Distanza di Hamming

DEFINIZIONE 93

Se $\mathbf{x}, \mathbf{y} \in F^n$, si definisce *distanza di Hamming* tra $\mathbf{x}$ e $\mathbf{y}$, e si denota con $d(\mathbf{x}, \mathbf{y})$, il numero di posizioni in cui le parole

$$\mathbf{x} = (x_1, x_2, \ldots, x_n) \text{ e } \mathbf{y} = (y_1, y_2, \ldots, y_n)$$

presentano lettere differenti, cioè

$$d(\mathbf{x}, \mathbf{y}) = \left|\{i \ : \ x_i \neq y_i, \ \ 1 \leq i \leq n\}\right|$$

La funzione d è una metrica su F^n, detta *metrica di Hamming*.

ESEMPIO 94

Risulta: $d(10101, 12210) = 4\,, \ \ d(11101, 10011) = 3\,,$

$$d(abcdef, afcbdb) = 4\,, \ \ d(0000000, 1111111) = 7\,.$$

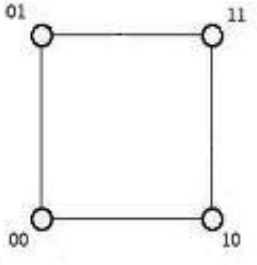
OSSERVAZIONE 95

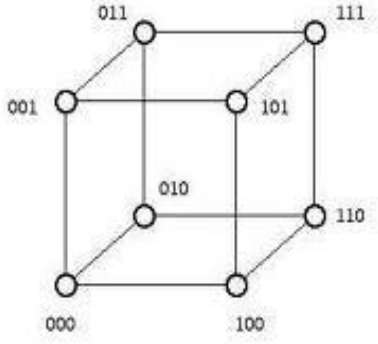
Per calcolare la distanza tra due parole di lunghezza n bisogna confrontare n coppie di lettere.

Distanza di Hamming

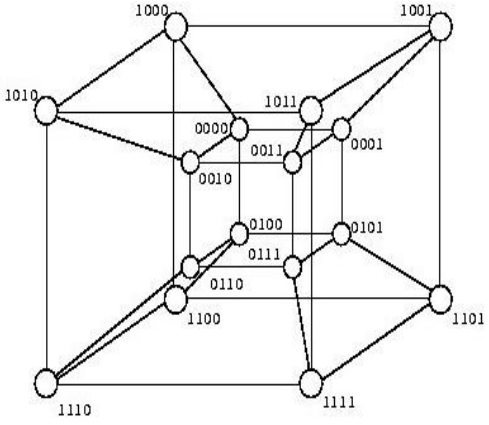
Le parole binarie di lunghezza n si possono rappresentare come i vertici di un ipercubo $n-$dimensionale. In questa rappresentazione la distanza tra due parole è uguale al numero minimo di lati che servono per unire i vertici corrispondenti alle parole assegnate.

Le figure seguenti sono le rappresentazioni grafiche di Z_2^2 e Z_2^3 rispettivamente come vertici di un quadrato e di un cubo.





Distanza di Hamming



In questa figura sono rappresentate le parole di Z_2^4 come vertici dell'ipercubo 4-dimensionale, proiettato nello spazio tridimensionale.

Distanza di Hamming

Ricordiamo che l'essere la distanza di Hamming una metrica su F^n significa che valgono le seguenti proprietà:
(1) $d(\mathbf{x}, \mathbf{y}) \geq 0$,
(2) $d(\mathbf{x}, \mathbf{y}) = 0 \quad \Leftrightarrow \quad \mathbf{x} = \mathbf{y}$,
(3) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$,
(4) $d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$ (*disuguaglianza triangolare*),
per ogni $\mathbf{x}, \mathbf{y}, \mathbf{z} \in F^n$.
Le proprietà (1),(2),(3) sono di immediata verifica. La proprietà (4) è conseguenza del fatto che la distanza $d(\mathbf{x}, \mathbf{y})$ tra due parole $\mathbf{x}, \mathbf{y} \in F^n$ è il minimo numero di lettere che bisogna modificare nella parola $\mathbf{x}$ per ottenere $\mathbf{y}$.

OSSERVAZIONE 96

La metrica di Hamming può definirsi su un qualsiasi sottoinsieme di F^n.

CONVENZIONE 97

Quando nel seguito useremo il termine distanza, intenderemo sempre distanza di Hamming.

DEFINIZIONE 98

Un codice C su un alfabeto F si dice *a blocchi* se le sue parole hanno tutte la stessa lunghezza; nel caso contrario si dice *a lunghezza variabile*. La comune lunghezza delle parole di un codice a blocchi si chiama *lunghezza del codice*.

DEFINIZIONE 99

Un codice su un alfabeto con q lettere che contenga esattamente M parole di lunghezza n prende il nome di $(n, M)-$*codice* $q-$*ario*, o semplicemente di $(n, M)-$*codice*, se q risulta chiaro dal contesto.
Nei casi $q = 2, 3$ il codice si dice rispettivamente *binario* e *ternario.*

ESEMPIO 100

Il codice

$$C = \{10101\,,\ 12210\,,\ 01202\,,\ 21020\}$$

è un $(5, 4)-$codice ternario.

Ipotesi di lavoro

Nel seguito prenderemo in considerazione soltanto codici a blocchi e useremo il termine *codice* come sinonimo di *codice a blocchi.* Inoltre, tranne avviso contrario, riterremo fissato un $(n, M)-$codice C su un alfabeto F con q lettere. C sarà sempre considerato come spazio metrico rispetto alla metrica di Hamming.

Spesso identificheremo il codice C con una matrice su F le cui righe sono le parole di C, preventivamente ordinate. Una tale matrice ha M righe ed n colonne e si dice *associata* a C. Due matrici associate ad uno stesso codice differiscono, quindi, per una permutazione delle righe.

ESEMPIO 101

Sia $C = \{10101\,,\ 12210\,,\ 01202\,,\ 21020\}$. Due matrici associate a C sono:

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 0 \\ 0 & 1 & 2 & 0 & 2 \\ 2 & 1 & 0 & 2 & 0 \end{bmatrix}, \quad \begin{bmatrix} 2 & 1 & 0 & 2 & 0 \\ 0 & 1 & 2 & 0 & 2 \\ 1 & 2 & 2 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

DEFINIZIONE 102

Si chiama *distanza minima* di un $(n, M)-$codice C l'intero $d = d(C)$ dato dalla più piccola distanza fra due parole distinte di C, cioè

$$d(C) := min\{d(\mathbf{x}, \mathbf{y}) \ : \ \mathbf{x}, \mathbf{y} \in C \ , \ \mathbf{x} \neq \mathbf{y}\}.$$

Un tale codice si dice anche un (n, M, d)-*codice* e gli interi n, M, d si dicono *parametri* del codice.

ESEMPIO 103

Per il codice $C = \{10101\ ,\ 12210\ ,\ 21021\ , 21020\}$, risulta

$$\begin{array}{ll} d(10101, 12210) = 4 & d(10101, 01201) = 4 \\ d(10101, 21020) = 5 & d(12210, 01202) = 4 \\ d(12210, 21021) = 5 & d(01202, 21020) = 4 \end{array}$$

e, pertanto, è $d = 4$.

Quanto costa il calcolo della distanza minima?

Per calcolare la distanza minima di un $(n, M)-$codice bisogna calcolare

$$\binom{M}{2} = \frac{M(M-1)}{2}$$

distanze tra due parole distinte di lunghezza n e, quindi, confrontare

$$n\binom{M}{2}$$

coppie di lettere.

OSSERVAZIONE 104

Vedremo che la conoscenza della distanza minima di un codice è indispensabile per stabilire la sua capacità di correggere e scoprire errori.

Esempio

Il codice binario di Hamming $Ham(3,2)$

Le righe della matrice

$$H(3,2) = \begin{bmatrix} 1&1&1&0&0&0&0 \\ 0&1&0&1&0&1&0 \\ 0&0&1&0&0&1&1 \\ 0&0&1&1&1&0&0 \\ 0&1&0&0&1&0&1 \\ 1&0&0&0&1&1&0 \\ 1&0&0&1&0&0&1 \\ 0&0&0&0&0&0&0 \\ 1&1&1&1&1&1&1 \\ 0&0&0&1&1&1&1 \\ 1&0&1&0&1&0&1 \\ 1&1&0&1&1&0&0 \\ 1&1&0&0&0&1&1 \\ 1&0&1&1&0&1&0 \\ 0&1&1&1&0&0&1 \\ 0&1&1&0&1&1&0 \end{bmatrix} \begin{matrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \mathbf{a}_3 \\ \mathbf{a}_4 \\ \mathbf{a}_5 \\ \mathbf{a}_6 \\ \mathbf{a}_7 \\ \mathbf{0} \\ \mathbf{1} \\ \mathbf{b}_1 \\ \mathbf{b}_2 \\ \mathbf{b}_3 \\ \mathbf{b}_4 \\ \mathbf{b}_5 \\ \mathbf{b}_6 \\ \mathbf{b}_7 \end{matrix}$$

costituiscono le parole di un $(7,16)$-codice: il *codice binario di Hamming* $Ham(3,2)$.

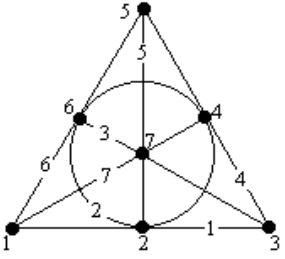
Per tali parole si ha:

$$d(\mathbf{0},\mathbf{a}_i) = 3, \quad d(\mathbf{0},\mathbf{b}_i) = 4, \quad d(\mathbf{0},\mathbf{1}) = 7,$$
$$d(\mathbf{a}_i,\mathbf{1}) = 4, \quad d(\mathbf{b}_i,\mathbf{1}) = 3, \quad d(\mathbf{a}_i,\mathbf{a}_j) = 4,$$
$$d(\mathbf{a}_i,\mathbf{b}_i) = 7, \quad d(\mathbf{a}_i,\mathbf{b}_j) = 3, \quad d(\mathbf{b}_i,\mathbf{b}_j) = 4.$$

per ogni $i \neq j$.

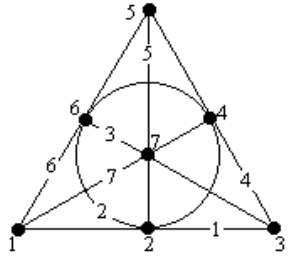
Risulta, pertanto, $d = 3$.

Le parole con esattamente tre bit uguali ad 1 del codice di Hamming $H(3,2)$ possono essere riguardate come i vettori caratteristici di sette sottoinsiemi d'ordine 3 di un insieme con 7 elementi, come mostra la figura seguente.

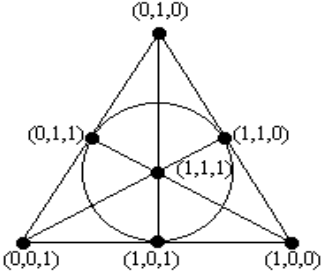


$$H(3,2) = \begin{bmatrix} 1&1&1&0&0&0&0 \\ 0&1&0&1&0&1&0 \\ 0&0&1&0&0&1&1 \\ 0&0&1&1&1&0&0 \\ 0&1&0&0&1&0&1 \\ 1&0&0&0&1&1&0 \\ 1&0&0&1&0&0&1 \\ 0&0&0&0&0&0&0 \\ 1&1&1&1&1&1&1 \\ 0&0&0&1&1&1&1 \\ 1&0&1&0&1&0&1 \\ 1&1&0&1&1&0&0 \\ 1&1&0&0&0&1&1 \\ 1&0&1&1&0&1&0 \\ 0&1&1&1&0&0&1 \\ 0&1&1&0&1&1&0 \end{bmatrix} \begin{matrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \mathbf{a}_3 \\ \mathbf{a}_4 \\ \mathbf{a}_5 \\ \mathbf{a}_6 \\ \mathbf{a}_7 \\ \mathbf{0} \\ \mathbf{1} \\ \mathbf{b}_1 \\ \mathbf{b}_2 \\ \mathbf{b}_3 \\ \mathbf{b}_4 \\ \mathbf{b}_5 \\ \mathbf{b}_6 \\ \mathbf{b}_7 \end{matrix}$$

La configurazione che si ottiene, considerando i sottoinsiemi i cui vettori caratteristici sono le parole di $Ham(3,2)$ con esattamente tre bit uguali ad 1, è quella formata dai vettori non nulli e dai sottospazi di dimensione 2 dello spazio vettoriale numerico Z_2^3 (*piano di Fano*).



Il piano di Fano



ESERCIZIO 105

Costruire il codice di Hamming $H(3,2)$, partendo dal piano di Fano.

Esempio

Le righe della matrice

$$H' = \begin{bmatrix} 0&0&0&0&0&0&0 \\ 1&1&0&1&0&0&1 \\ 0&1&0&1&0&1&0 \\ 1&0&0&0&0&1&1 \\ 1&0&0&1&1&0&0 \\ 0&1&0&0&1&0&1 \\ 1&1&0&0&1&1&0 \\ 0&0&0&1&1&1&1 \\ 1&1&1&0&0&0&0 \\ 0&0&1&1&0&0&1 \\ 1&0&1&1&0&1&0 \\ 0&1&1&0&0&1&1 \\ 0&1&1&1&1&0&0 \\ 1&0&1&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 1&1&1&1&1&1&1 \end{bmatrix} \begin{matrix} \mathbf{0} \\ \mathbf{b}_1 \\ \mathbf{a}_1 \\ \mathbf{a}_2 \\ \mathbf{a}_3 \\ \mathbf{a}_4 \\ \mathbf{b}_2 \\ \mathbf{b}_3 \\ \mathbf{a}_5 \\ \mathbf{a}_6 \\ \mathbf{b}_4 \\ \mathbf{b}_5 \\ \mathbf{b}_6 \\ \mathbf{b}_7 \\ \mathbf{a}_7 \\ \mathbf{1} \end{matrix}$$

rappresentano le soluzioni sul campo Z_2 del sistema lineare

$X_4 + X_5 + X_6 + X_7 = 0$,
$X_2 + X_3 + X_6 + X_7 = 0$,
$X_1 + X_3 + X_5 + X_7 = 0$.

e costituiscono le parole di un $(7, 16)$-codice per le cui parole si ha:

$$d(\mathbf{0}, \mathbf{a}_i) = 3, \quad d(\mathbf{0}, \mathbf{b}_i) = 4, \quad d(\mathbf{0}, \mathbf{1}) = 7,$$
$$d(\mathbf{a}_i, \mathbf{1}) = 4, \quad d(\mathbf{b}_i, \mathbf{1}) = 3, \quad d(\mathbf{a}_i, \mathbf{a}_j) = 4,$$
$$d(\mathbf{a}_i, \mathbf{b}_i) = 7, \quad d(\mathbf{a}_i, \mathbf{b}_j) = 3, \quad d(\mathbf{b}_i, \mathbf{b}_j) = 4.$$

per ogni $i \neq j$. Risulta, pertanto, $d = 3$.

Vedremo in seguito che, dal punto di vista dei codici lineari, H' può considerarsi equivalente al codice $Ham(3, 2)$.

Disuguaglianza di Singleton

PROPOSIZIONE (Disuguaglianza di Singleton) **106**

Per ogni $(n, M, d)-$*codice* $q-$*ario* C, *risulta*

$$M \leq q^{n-d+1}\,. \tag{21}$$

DIMOSTRAZIONE

L'applicazione $(a_1, a_2, .., a_n) \in C \rightarrow (a_1, a_2, .., a_{n-d+1}) \in F^{n-d+1}$ è iniettiva, altrimenti C conterrebbe parole a distanza minore di d, avendosi $d((a_1, .., a_{n-d+1}, b_{n-d+2}, .., b_n), (a_1, .., a_{n-d+1}, c_{n-d+2}, .., c_n)) < d$.

ESEMPIO **107**

Un codice binario con $n = 4$ e $d = 2$ può avere al più $M = 8$ parole. Un codice con questi parametri è il seguente

$$\{0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111\}.$$

DEFINIZIONE 108

Diciamo che il codice C è $k-$*sistematico*, o semplicemente *sistematico*, se in una delle sue matrici associate esistono k colonne di posto $i_1, i_2, ..., i_k$ tali che, l'applicazione

$$(a_1, a_2, \ldots, a_n) \in C \rightarrow (a_{i_1}, a_{i_2}, \ldots, a_{i_k}) \in F^k$$

è biunivoca.
In queste ipotesi, gli interi $i_1, i_2, ..., i_k$ si chiamano *posti di informazione*, l'intero $n - k$ prende il nome di *ridondanza* di C e si dicono *ridondanti* o *di controllo* le lettere delle parole di C che occupano posizioni diverse da $i_1, i_2, ..., i_k$.

ESEMPIO 109

Il codice $C = \{000, 101, 011, 111\}$ è $2-$sistematico. I posti 1,2 sono di informazione. I posti 1,3 e 2,3 non sono di informazione.

OSSERVAZIONE 110

Se C è $k-$sistematico si ha

$$|C| = q^k.$$

Se, inoltre, $i_1, i_2, ..., i_k$ sono posti di informazione, allora, per ogni $k-$pla $\alpha = (\alpha_1, \alpha_2, ..., \alpha_k)$ di lettere di F, esiste un'unica parola $f(\alpha) = (a_1, a_2, \ldots, a_n)$ di C per cui risulta

$$a_{i_1} = \alpha_1,\ a_{i_2} = \alpha_2, ... \ , a_{i_k} = \alpha_k.$$

La funzione $f : F^k \longrightarrow C$ così definita è, dunque, una codifica di F^k su F mediante C.

OSSERVAZIONE 111

I codici $k-$sistematici di lunghezza n si prestano a codificare insiemi di q^k messaggi mediante parole di lunghezza n, riservando $n - k$ lettere per il controllo di ogni messaggio codificato.

OSSERVAZIONE 112

Un codice $k-$sistematico non può essere $h-$sistematico, con $k \neq h$.

ESEMPIO 113

Il codice

$$C = \{0000, 1100, 1001, 0101, 0011, 0110, 1111\}$$

non è sistematico.

ESEMPIO 114

Il codice $C = \{00000, 10100, 01100, 00011, 11000, 10111, 01111, 11011\}$ è $3-$sistematico. Suoi posti di informazione sono il primo, il secondo e il quarto. Una codifica naturale di F^3, $F = \{0, 1\}$, mediante C è

$$\begin{array}{lll} 000 \to 00000 & 100 \to 10100 & 010 \to 01100 \\ 001 \to 00011 & 110 \to 11000 & 101 \to 10111 \\ 011 \to 01111 & 111 \to 11011 & \end{array}$$

Il codice di Hamming è $4-$sistematico:

$$H(3,2) = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

PROPOSIZIONE (Disuguaglianza di Singleton per codici sistematici) **115**

Se C è un $(n, M, d)-$codice $k-$sistematico si ha

$$d \leq n - k + 1\,. \tag{22}$$

DIMOSTRAZIONE

Dalla disuguaglianza di Singleton, $M \leq q^{n-d+1}$, risulta $|C| = q^k \leq q^{n-d+1}$, da cui l'asserto.

OSSERVAZIONE 116

Si noti che la (22) non dipende da q.

DEFINIZIONE 117

Un $(n, M, d)-$codice $k-$sistematico C si dice *MDS* (*maximum distance separable*) o, *ottimale*, se risulta $d = n - k + 1$.

Codici sistematici e codici *MDS*

PROPOSIZIONE 118

Un $(n, M, d)-$codice $k-$sistematico è MDS se, e solo se, ogni $k-$posti sono di informazione.

DIMOSTRAZIONE

C è *MDS* se, e solo se, $d = n - k + 1$. Allora l'asserto segue dall'osservazione che due parole distinte di C hanno le stesse lettere in k posti fissati se, e solo se, la loro distanza è minore o uguale di di $n - k$.

ESEMPIO 119

Il codice $\{0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111\}$ è *MDS*.

2. Decodifica di minima distanza e codici correttori

indice

DEFINIZIONE 120

Per ogni $\mathbf{x} \in F^n$ e per ogni intero $r > 0$, si definisce *sfera (di Hamming) di centro* $\mathbf{x}$ *e raggio* r l'insieme

$$S(\mathbf{x}, r) := \{\mathbf{y} \in F^n \quad : \quad d(\mathbf{x}, \mathbf{y}) \leq r\}.$$

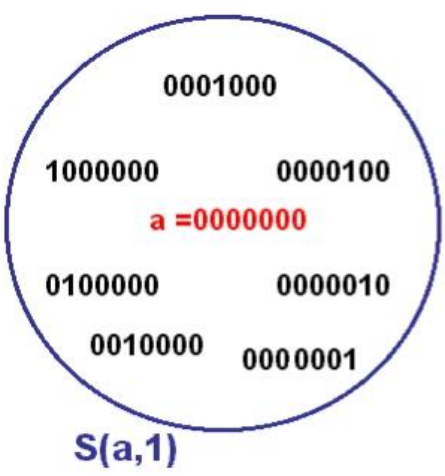
La sfera $S(\mathbf{x}, r)$ si denota anche con $S_r(\mathbf{x})$ o con $B_r(\mathbf{x})$.
L'insieme

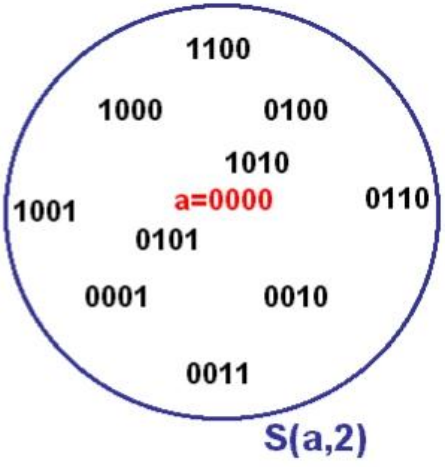
$$\Sigma(\mathbf{x}, r) := \{\mathbf{y} \in F^n \quad : \quad d(\mathbf{x}, \mathbf{y}) = r\}$$

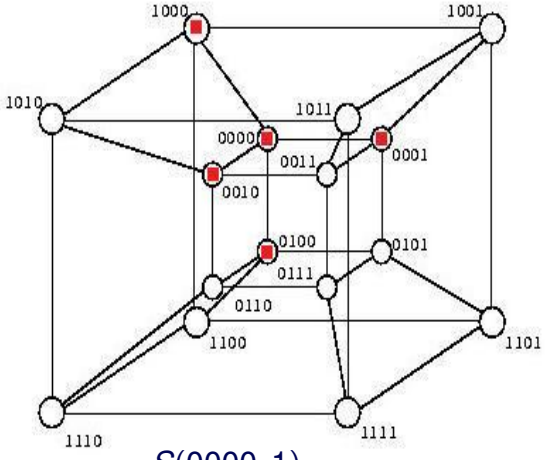
prende il nome di *superficie sferica di centro* $\mathbf{x}$ *e raggio* r. La superficie sferica $\Sigma(\mathbf{x}, r)$ si denota anche con $\Sigma_r(\mathbf{x})$.

PROPOSIZIONE 121

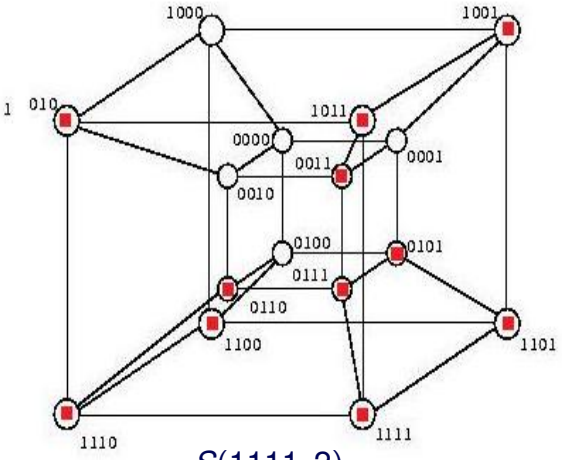
$$\begin{cases} \Sigma(\mathbf{x}, r) \cap \Sigma(\mathbf{x}, r') = \emptyset, \quad r \neq r', \quad r, r' \leq n \\ S(\mathbf{x}, r) = \bigcup_{0 \leq s \leq r} \Sigma(\mathbf{x}, s) \end{cases} \tag{23}$$


0001000
1000000
0000100
a =0000000
0100000
0000010
0010000
0000001
S(a,1)


1100
1000
0100
1010
1001
a=0000
0110
0101
0001
0010
0011
S(a,2)



$S(0000, 1)$



$S(1111, 2)$

Le parole delle due sfere sono rappresentate dai punti rossi.

Numero di parole in una sfera di Hamming

PROPOSIZIONE 122

Una sfera di raggio r, $0 \leq r \leq n$, in F^n contiene esattamente

$$\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{r}(q-1)^r$$

parole.

DIMOSTRAZIONE

Le parole a distanza s da una fissata parola $\mathbf{x}$ si ottengono modificando arbitrariamente s lettere di $\mathbf{x}$ e quindi sono esattamente $\binom{n}{s}(q-1)^s$. Dalle (23) segue allora l'asserto.

ESEMPIO 123

Per la parola binaria 000, risulta:

$$S_2(000) = \{000, 100, 010, 001, 110, 101, 011\},$$

$$\Sigma_0(000) = \{000\}, \quad \Sigma_1(000) = \{100, 010, 001\},$$

$$\Sigma_2(000) = \{110, 101, 011\}.$$

ESEMPIO 124

Per la parola ternaria 012, risulta:

$$|S_2(012)| = \binom{3}{0} + \binom{3}{1}2 + \binom{3}{2}2^2 = 19.$$

Decodifica di minima distanza

DEFINIZIONE 125

Sia C un $(n, M)-$codice $q-$ario su un alfabeto F. Una decodifica di C

$$\pi : \mathbf{y} \in F^n \rightarrow \mathbf{z} = \pi(\mathbf{y}) \in C$$

tale che $d(\mathbf{y}, \mathbf{z}) \leq d(\mathbf{y}, \mathbf{a})$, per ogni $\mathbf{a} \in C \setminus \{\mathbf{z}\}, \mathbf{y} \in F^n$, si dice di *minima distanza* (*nearest-neighbour decoding*).

OSSERVAZIONE 126

Una decodifica di minima distanza di C associa ad ogni parola di C la parola stessa.

ESEMPIO 127

Sia $C = \{000, 011, 101, 110\}$. La seguente decodifica di C è di minima distanza:

$$000 \rightarrow 000\,,\ 100 \rightarrow 000\,,\ 010 \rightarrow 011\,,\ 001 \rightarrow 101\,,$$

$$110 \rightarrow 110\,,\ 101 \rightarrow 101\,,\ 011 \rightarrow 011\,,\ 111 \rightarrow 011\,.$$

Scoprire errori

DEFINIZIONE 128

Si dice che il codice C *scopre* h errori se la sfera $S(\mathbf{a}, h)$ ha in comune con C la sola parola $\mathbf{a}$, per ogni $\mathbf{a} \in C$ o, equivalentemente,

$$\mathbf{x} \in F^n\,,\ \mathbf{a} \in C\,,\ 0 < d(\mathbf{x}, \mathbf{a}) \leq h\,,\ \Rightarrow \mathbf{x} \notin C.$$

OSSERVAZIONE 129

La definizione appena data è motivata dalla seguente osservazione. Supponiamo che su una parola $\mathbf{a} \in C$, trasmessa attraverso un canale, vengano commessi al più $h > 0$ errori e sia $\mathbf{x} \in F^n$ la nuova parola. Allora, essendo $d(\mathbf{x}, \mathbf{a}) \leq h$, $\mathbf{x}$ non è una parola di C e l'errore viene rilevato.

PROPOSIZIONE 130

Un $(n, M)-$codice C scopre h errori se, e solo se, risulta

$$d \geq h + 1.$$

Ne segue anche che il massimo numero di errori che C può scoprire è $d-1$.

DEFINIZIONE 131

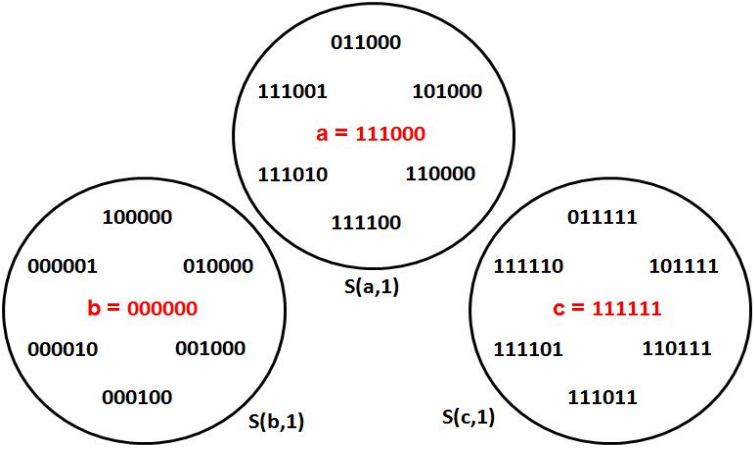
Si dice che il codice C *corregge* h errori se due qualsiasi sfere di raggio h con centri in parole distinte di C sono ad intersezione vuota o, equivalentemente,

$$\mathbf{x} \in F^n\,,\ \mathbf{a} \in C\,,\ d(\mathbf{x},\mathbf{a}) \leq h \Rightarrow d(\mathbf{x},\mathbf{b}) > h,\ \forall \mathbf{b} \in C \setminus \{\mathbf{a}\}.$$

OSSERVAZIONE 132

Supponiamo che su una parola $\mathbf{a} \in C$ vengano commessi al più h errori e sia $\mathbf{x} \in F^n$ la nuova parola. Allora, se C corregge h errori, $\mathbf{a}$ è l'unica parola del codice C a distanza minore o uguale di h da $\mathbf{x}$ e ogni decodifica di minima distanza corregge l'errore.

Il codice $C = \{000000\,,\ 1111111,,\ 111000\}$ ha distanza minima 3 e, quindi, corregge un errore. Questo significa che le sfere con centro le parole del codice e raggio 1 sono a due a due disgiunte.



DEFINIZIONE 133

Il massimo numero di errori che un codice C può correggere viene denotato con e e si chiama anche *raggio di impacchettamento di C*; in questo caso C si dice *e−correttore*.

PROPOSIZIONE 134

Un $(n, M)-$codice C corregge h errori se, e solo se, risulta

$$d \geq 2h + 1.$$

Ne segue anche che, C è e−correttore se, e solo se, risulta

$$d = 2e + 1 \quad o \quad d = 2e + 2,$$

a seconda che d sia dispari o pari, rispettivamente.

OSSERVAZIONE 135

Il raggio di impacchettamento e di un codice C coincide col più grande intero r per cui due sfere di raggio r con centro in due qualsiasi parole distinte di C sono ad intersezione vuota.

OSSERVAZIONE 136

Supponiamo di trasmettere le parole di un $(n, M)-$codice $e-$correttore C attraverso un canale che commette al più e errori su ogni parola di lunghezza n. Allora ogni parola ricevuta appartiene all'unione delle sfere di centro le parole di C e raggio e ed è decodificata correttamente da una qualsiasi decodifica di minima distanza.

DEFINIZIONE 137

Il *raggio di copertura* di un (n, M)-codice C è il più piccolo intero s per cui le sfere di raggio r e centro le parole di C costituiscono un ricoprimento dell'insieme delle parole di lunghezza n, cioè

$$F^n = \bigcup_{a \in C} S(\mathbf{a}, r)\,.$$

OSSERVAZIONE 138

Se un codice C di lunghezza n ha raggio di copertura s, allora ogni parola in F^n appartiene ad almeno una sfera di raggio s con centro in una parola di C.

3. Codici perfetti e disuguaglianza di Hamming

indice

PROPOSIZIONE (Disuguaglianza di Hamming) **139**

Per ogni $(n, M)-$*codice* C *che sia* $e-$*correttore, risulta*

$$M\left[\binom{n}{0}+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{e}(q-1)^e\right]\leq q^n$$

DIMOSTRAZIONE

Le sfere di centro le parole di C e raggio e sono a due a due disgiunte. L'unione di tali sfere contiene un numero di parole pari a quello che compare al primo membro della disuguaglianza e tale numero, ovviamente, non supera il numero q^n di tutte le parole di lunghezza n.

DEFINIZIONE 140

La differenza tra il secondo e il primo membro della precedente disuguaglianza si chiama *difetto* del codice e si denota con $\delta = \delta(C)$.

DEFINIZIONE 141

Un $(n, M)-$codice $e-$correttore si dice *perfetto* se ha difetto 0, cioè

$$M\left[\binom{n}{0}+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{e}(q-1)^e\right]=q^n.$$

OSSERVAZIONE 142

Un codice per cui il raggio di impacchettamento coincide con quello di copertura, cioè $e = s$, risulta perfetto.
In altre parole, un codice $e-$correttore di lunghezza n è perfetto se e, solo se, le sfere di raggio e con centro le parole di C costituiscono una partizione di F^n e, quindi,

$$F^n=\bigcup_{a\in C} S(\mathbf{a}, e)\,.$$

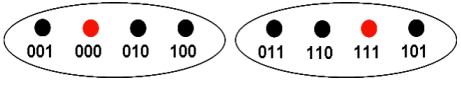
Questo significa che per ogni parola $\mathbf{y} \in F^n$ esiste un'unica parola $\mathbf{a} \in C$ tale che $\mathbf{y} \in S(\mathbf{a}, e)$.

OSSERVAZIONE 143

Supponiamo di trasmettere le parole di un $(n, M)-$codice perfetto $e-$correttore C attraverso un canale che commette al più e errori su ogni parola di lunghezza n. Allora, in una decodifica di minima distanza, ogni parola ricevuta è decodificata correttamente.

ESEMPIO 144

Il codice $C = \{000\,,\ 111\}$ di distanza minima $d = 3$ è perfetto.



ESEMPIO 145

Il codice $C = \{10101\,,\ 12210\,,\ 01202\,,\ 10100\}$ di distanza minima $d = 1$ non è perfetto:

$$4\left[\binom{5}{0}\right] = 4 < 3^5.$$

Il suo difetto è dato da $\delta = 243 - 4 = 239$.

OSSERVAZIONE 146

La proprietà di un codice di essere perfetto dipende esclusivamente dai suoi parametri. Questo significa che, se un $(n, M, d)-$codice C è perfetto, ogni codice con gli stessi parametri di C è anch'esso perfetto.

PROPOSIZIONE 147

Se C è un $(n, M, d)-$codice perfetto, allora d è dispari.

DIMOSTRAZIONE

Se $d = 2e + 2$ e $\mathbf{a}$ è una parola di C, una parola $\mathbf{x} \in F^n$ a distanza $e + 1$ da $\mathbf{a}$, in forza della disuguaglianza triangolare, è a distanza maggiore di e da ogni parola $\mathbf{b}$ ($\neq \mathbf{a}$) di C e, quindi, C non è perfetto:

$$2e + 2 \leq d(\mathbf{a}, \mathbf{b}) \leq d(\mathbf{a}, \mathbf{x}) + d(\mathbf{x}, \mathbf{b}) = e + 1 + d(\mathbf{x}, \mathbf{b})$$

$$\Rightarrow d(\mathbf{x}, \mathbf{b}) \geq e + 1 \, .$$

ESEMPI 148

- Il codice $C = F^n$ è perfetto ($e = 0$):

$$q^n \left[\binom{n}{0} \right] = q^n.$$

- I codici contenenti una sola parola sono perfetti ($e = n$):

$$1 \left[\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{n}(q-1)^n \right] = q^n.$$

- I codici di ripetizione binari (due parole: una con tutti 0 e l'altra con tutti 1) di lunghezza dispari $n = 2e + 1$ sono perfetti:

$$2 \left[\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{\frac{n-1}{2}} \right] = 2 \cdot 2^{n-1} = 2^n.$$

DEFINIZIONE 149

I codici dei tre esempi precedenti vengono detti *codici perfetti banali*.

Esempio di codice perfetto

Ricordiamo che le righe della matrice

$$H(3,2) = \begin{bmatrix} 1&1&1&0&0&0&0 \\ 0&1&0&1&0&1&0 \\ 0&0&1&0&0&1&1 \\ 0&0&1&1&1&0&0 \\ 0&1&0&0&1&0&1 \\ 1&0&0&0&1&1&0 \\ 1&0&0&1&0&0&1 \\ 0&0&0&0&0&0&0 \\ 1&1&1&1&1&1&1 \\ 0&0&0&1&1&1&1 \\ 1&0&1&0&1&0&1 \\ 1&1&0&1&1&0&0 \\ 1&1&0&0&0&1&1 \\ 1&0&1&1&0&1&0 \\ 0&1&1&1&0&0&1 \\ 0&1&1&0&1&1&0 \end{bmatrix} \begin{matrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \mathbf{a}_3 \\ \mathbf{a}_4 \\ \mathbf{a}_5 \\ \mathbf{a}_6 \\ \mathbf{a}_7 \\ \mathbf{0} \\ \mathbf{1} \\ \mathbf{b}_1 \\ \mathbf{b}_2 \\ \mathbf{b}_3 \\ \mathbf{b}_4 \\ \mathbf{b}_5 \\ \mathbf{b}_6 \\ \mathbf{b}_7 \end{matrix}$$

costituiscono le parole del $(7, 16, 3)$-*codice binario di Hamming* $Ham(3, 2)$.

Poiché risulta

$$16\left[\binom{7}{0} + \binom{7}{1}(2-1)\right] = 2^4 \times 2^3 = 2^7,$$

si ha che $Ham(3, 2)$ è un codice perfetto.

Partizione di Z_2^7 nelle sfere di centro le parole di $Ham(3,2)$ e raggio 1

1110000	0101010	0010011	0011100	0100101	1000110	1001001	0000000
0110000	1101010	1010011	1011100	1100101	0000110	0001001	1000000
1010000	0001010	0110011	0111100	0000101	1100110	1101001	0100000
1100000	0111010	0000011	0001100	0110101	1010110	1011001	0010000
1111000	0100010	0011011	0010100	0101101	1001110	1000001	0001000
1110100	0101110	0010111	0011000	0100001	1000010	1001101	0000100
1110010	0101000	0010001	0011110	0100111	1000100	1001011	0000010
1110001	0101011	0010010	0011101	0100100	1000111	1001000	0000001

0001111	1010101	1101100	1100011	1011010	0111001	0110110	1111111
1001111	0010101	0101100	0100011	0011010	1111001	1110110	0111111
0101111	1110101	1001100	1000011	1111010	0011001	0010110	1011111
0011111	1000101	1111100	1110011	1001010	0101001	0100110	1101111
0000111	1011101	1100100	1101011	1010010	0110001	0111110	1110111
0001011	1010001	1101000	1100111	1011110	0111101	0110010	1111011
0001101	1010111	1101110	1100001	1011000	0111011	0110100	1111101
0001110	1010100	1101101	1100010	1011011	0111000	0110111	1111110

$$2^3 2^4 = 2^7$$

4. Algoritmi di decodifica

indice

Algoritmo generico per decodifica incompleta

DATI:

Un $(n, M)-$codice C su un alfabeto F ed una parola $\mathbf{y} \in F^n$ da decodificare.

ALGORITMO 1

1. Si ponga $t = 0$.
2. Se $D_t = S(\mathbf{y}, t) \cap C \neq \emptyset$ si distinguano due casi:
   a. se $D_t = \{\mathbf{y}\}$, si restituiscano t e $\mathbf{y}$;
   b. se $\mid D_t \mid > 1$, si restituisca t
3. Si ponga $t = t + 1$.
4. Si torni al punto 2.

RISULTATO 150

Sia e il più piccolo intero non negativo tale che $D_e = S(\mathbf{y}, e) \cap C \neq \emptyset$. Allora:
- se esiste un unico $\mathbf{z} \in C$ per cui è $d(\mathbf{z}, \mathbf{y}) = e$, l'algoritmo rileva e errori e li *corregge automaticamente,* decodificando $\mathbf{y}$ con $\mathbf{z}$ **(decodifica completa)**;
- nel caso contrario l'algoritmo segnala che la parola $\mathbf{y}$ è affetta da almeno e errori, che non è possibile correggere **(decodifica incompleta)**.

ESEMPIO 151

Si consideri il codice $1-$correttore $C = \{00000, 10110, 01101, 11011\}$. Di seguito riportiamo la decodifica di alcune parole mediante l'ALGORITMO 1:

$$10000 \to 00000\,,\ 01111 \to 01101\,,\ 10001 \to 2, 11000 \to 2$$

OSSERVAZIONE 152

Se si usa un canale di trasmissione che commette al più e errori su ogni parola $q-$aria di lunghezza n e se C è $e-$correttore, l'ALGORITMO 1 è di minima distanza e decodifica automaticamente e correttamente ogni parola in ricezione (Osservazione 142).

OSSERVAZIONE 153

Senza particolari ipotesi sul codice C, il calcolo degli insiemi D_t nell'ALGORITMO 1, richiede un notevole dispendio di tempo: bisogna enumerare tutte le parole di C e controllare quali di queste hanno distanza da $\mathbf{x}$ non superiore ad e.

Algoritmo generico per decodifica incompleta

DATI:

Un $(n, M)-$codice $e-$correttore C su un alfabeto F ed una parola $\mathbf{y} \in F^n$ da decodificare.

ALGORITMO 2

1. Si ponga $D = S(\mathbf{y}, e)$.
2. Se $D \cap C = \{\mathbf{z}\}$ si restituiscano $d(\mathbf{y}, \mathbf{z})$ e $\mathbf{z}$.
3. Se $D \cap C = \emptyset$ si segnali che si sono verificati almeno $e + 1$ errori.

RISULTATO 154

Se $D \cap C = \{\mathbf{z}\}$, l'algoritmo rileva $d(\mathbf{y}, \mathbf{z})$ errori e li *corregge automaticamente,* decodificando $\mathbf{y}$ con $\mathbf{z}$; **(decodifica completa).**
Nel caso contrario l'algoritmo segnala che la parola $\mathbf{y}$ è affetta da almeno $e + 1$ errori, che non è possibile correggere **(decodifica incompleta)**.

Sia C un $(n, M)-$codice $q-$ario $e-$correttore e distribuiamo tutte le parole di F^n in una tabella

$$\Sigma = (\sigma_{ij})$$

con M colonne in modo che siano soddisfatte le seguenti proprietà:

(i) *la prima riga contiene tutte le parole di* C;
(ii) *per ogni coppia* (i, j) *di indici è*

$$d(\sigma_{ij}, \sigma_{1j}) \leq d(\sigma_{ij}, \mathbf{a}),$$

per ogni $\mathbf{a} \in C$.

Una tabella Σ così costruita prende il nome di *tabella standard* di C.

Tabelle per decodifica di minima distanza

ESEMPIO 155

Il $(4,4)-$codice binario

$$C = \{(0,0,0,0),(1,0,1,1),(0,1,0,1),(1,1,1,0)\}$$

ha la seguente tabella standard

$$\Sigma = \begin{matrix} 0000 & 1011 & 0101 & 1110 \\ 1000 & 0011 & 1101 & 0110 \\ 0100 & 1111 & 0001 & 1010 \\ 0010 & 1001 & 0111 & 1100 \end{matrix}$$

Tabelle per decodifica di minima distanza

ESEMPIO 156

Il $(5,4)-$codice binario

$$C = \{(0,0,0,0,0),(1,0,1,1,0),(0,1,0,1,1),(1,1,1,0,1)\}$$

ha la seguente tabella standard

$$\Sigma = \begin{array}{cccc} 00000 & 10110 & 01011 & 11101 \\ 10000 & 00110 & 11011 & 01101 \\ 01000 & 11110 & 00011 & 10101 \\ 00100 & 10010 & 01111 & 11001 \\ 00010 & 10100 & 01001 & 11111 \\ 00001 & 10111 & 01010 & 11100 \\ 10001 & 00111 & 10100 & 01100 \\ 11000 & 01110 & 10011 & 00101 \end{array}.$$

Decodifica con tabella

DATI: 157

Un $(n, M)-$codice C su un alfabeto F, una tabella standard di C ed una parola $\mathbf{y} \in F^n$ da decodificare.

ALGORITMO 3 158

1. scorrere la tabella standard, iniziando dal primo elemento della prima riga e continuando in successione, fino a trovare la parola ricevuta $\mathbf{y}$.
2. decodificare $\mathbf{y}$ come la prima parola della colonna della tabella cui $\mathbf{y}$ appartiene.

RISULTATO 159

Una decodifica di minima distanza.

OSSERVAZIONE 160

Se si usa un canale di trasmissione che commette al più e errori su ogni parola $q-$aria di lunghezza n e se C è $e-$correttore, l'ALGORITMO 3 decodifica automaticamente e correttamente ogni parola in ricezione.

Esempio di decodifica con tabella

Il $(5,4)-$codice binario $C = \{(0,0,0,0,0),\ (1,0,1,1,0),\ (0,1,0,1,1),\ (1,1,1,0,1)\}$ ha distanza minima 3 e, quindi, corregge un solo errore; una sua tabella standard è

$$\Sigma = \begin{array}{cccc} 00000 & 10110 & 01011 & 11101 \\ 10000 & 00110 & 11011 & 01101 \\ 01000 & 11110 & 00011 & 10101 \\ 00100 & 10010 & 01111 & 11001 \\ 00010 & 10100 & 01001 & 11111 \\ 00001 & 10111 & 01010 & 11100 \\ \hline 10001 & 00111 & 10100 & 01100 \\ 11000 & 01110 & 10011 & 00101 \end{array}$$

Se si usa un canale di trasmissione che commette al più un errore su ogni parola binaria di lunghezza 5, l'ALGORITMO 3 decodifica automaticamente e correttamente ogni parola di lunghezza 5 in ricezione.

Si noti, per esempio, che la parola 01100 ha distanza maggiore di 1 da ogni parola di C e si ottiene mediante due errori da 00000 e da 11101. Tale parola non può, quindi, essere decodificata correttamente dal nostro algoritmo.

5. Il problema fondamentale della teoria dei codici

indice

Ipotesi di lavoro

- Riterremo assegnato un alfabeto F con q lettere.
- L'insieme $\mathcal{M}$ dei messaggi sarà identificato con l'insieme F^k di tutte le parole di lunghezza k.
- I messaggi in $\mathcal{M} = F^k$ saranno codificati mediante un $(n, M)-$codice C sull'alfabeto F; di conseguenza avremo

$$|\mathcal{M}| = q^k \leq |C| = M \leq q^n \quad e \quad k \leq n, .$$

DEFINIZIONE 161

Si definiscono *tasso di informazione* $R(C)$, *efficienza* $R(n,k)$ e *ridondanza* $r(n,k)$ di C rispetto a $\mathcal{M}$ i seguenti numeri reali

$$R(C) = \frac{\log_q M}{n}\,,\ R(k,n) = \frac{k}{n}\,,\ \ r(n,k) = n-k\,,$$

rispettivamente

OSSERVAZIONE 162

l'efficienza di C rispeto a $\mathcal{M}$ è al più 1 e non può superare il tasso di informazione di C, cioè:

$$\frac{k}{n} = R(k,n) \leq R(C) = \frac{\log_q M}{n} \leq 1\,.$$

Esempio

Siano $F = \{0, 1\}$, $\mathcal{M} = F^2$ e

$$C = \{00000, 10110, 01011, 11101\}.$$

Per una qualsiasi codifica di $\mathcal{M}$ mediante il codice C, risulta

$$R(2,5) = \frac{2}{5}\,, \quad r(2,5) = 3\,.$$

Quelle che seguono sono due possibili codifiche di $\mathcal{M}$ mediante C :

$$\begin{array}{lcl} 00 & \mapsto & 00000 \\ 10 & \mapsto & 10110 \\ 01 & \mapsto & 11101 \\ 11 & \mapsto & 01011 \end{array} \qquad \begin{array}{lcl} 00 & \mapsto & 00000 \\ 10 & \mapsto & 10110 \\ 01 & \mapsto & 01011 \\ 11 & \mapsto & 11101 \end{array} .$$

Problema centrale

OSSERVAZIONE 163

È chiaro che la possibilità di correggere errori ha un costo: al crescere della ridondanza o, equivalentemente, al diminuire dell'entropia del sistema di comunicazione, corrisponde un aumento della capacità di correggere errori!

PROBLEMA 164

Costruire codici tali che, per ogni fissata ridondanza,

1. correggano il maggior numero possibile di errori,
2. esistano algoritmi efficienti per la loro codifica e la loro decodifica.

Problema fondamentale della teoria dei codici

Un "*buon*" codice dovrebbe avere:

- lunghezza *n abbastanza piccola* per permettere una trasmissione veloce delle sue parole;
- un numero *M* di parole *abbastanza grande* per codificare una buona quantità di messaggi;
- distanza minima *abbastanza grande* (cioè molta ridondanza) per correggere il maggior numero possibile di errori.

Queste richieste sono tra loro contrastanti e, di conseguenza, la ricerca di "buoni" codici richiede la valutazione del rapporto costi-benefici al variare di questi parametri. In particolare, è importante ottimizzare uno dei parametri avendo preventivamente fissato gli altri due.

Quest'ultimo tipo di problema va sotto il nome di *problema fondamentale della teoria dei codici*.

DEFINIZIONE 165

Fissati n e d, si denota con $A_q(n,d)$ il più grande intero M per cui esiste un $(n,M,d)-$codice $q-$ario.

CONVENZIONE 166

Nel seguito assumeremo che il problema fondamentale della teoria dei codici consista proprio nel calcolo della funzione $A_q(n,d)$

OSSERVAZIONE 167

Lo studio della funzione $A_q(n,d)$ è un problema estremamente difficile. Al momento si conosce il valore di $A_q(n,d)$ solo in pochi casi. Calcoleremo, per esempio, $A_q(4,3)$ mediante lo studio di alcune matrici speciali dette *quadrati latini.*

PROPOSIZIONE 168

Si ha:

$$A_q(n,1) = |F^n| = q^n\,, \quad A_q(n,n) = |F| = q\,. \tag{24}$$

DIMOSTRAZIONE

La condizione $d = 1$ impone soltanto che le parole di C siano tutte distinte fra loro e quindi il massimo valore di M si ottiene per $C = F^n$, cioè la prima delle (24).

Se, invece, abbiamo $d = n$,le lettere che figurano in una fissata posizione nelle parole di C devono essere a due a due distinte e quindi $A_q(n,n) \leq q$. D'altra parte il codice $C(F,n) = \{(a,a,...,a) \quad : \quad a \in F\}$ contiene esattamente q parole e gode della proprietà richiesta; abbiamo così la seconda delle (24).

DEFINIZIONE 169

Il codice $C(F,n)$ si chiama *codice di ripetizione $q-$ario di lunghezza n* o anche *(n,q,n)-codice di ripetizione su F*.

ESERCIZIO 170

Posto $d = 2e+1$ o $d = 2e+2$, provare che

$$A_q(n,d)\left[\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{e}(q-1)^e\right] \leq q^n.$$

Provare, inoltre, che l'uguaglianza può aversi solo nel caso d dispari.

PROPOSIZIONE 171

$$A_q(n,d)\left[\binom{n}{0} + \binom{n}{1}(q-1) + \cdots + \binom{n}{d-1}(q-1)^{d-1}\right] \geq q^n.$$

(Disuguaglianza di Gilbert-Varshamov)

DIMOSTRAZIONE

Sia C un $(n, M, d)-$codice con $M = A_q(n,d)$. Se la disuguaglianza fosse falsa, esisterebbe una parola $\mathbf{x}$ a distanza maggiore di $d-1$ da tutte le parole di C. Allora aggiungendo $\mathbf{x}$ a C si otterrebbe un $(n, M+1, d)-$codice, il che è assurdo.

6. Quadrati latini e $A_q(4,3)$

indice

Il problema dei 36 ufficiali di Eulero

Nel 1782 *Leonard Euler* pose il seguente

PROBLEMA 172

Supponiamo di avere 36 *ufficiali appartenenti a* 6 *diversi reggimenti, ognuno dei quali sia rappresentato da* 6 *ufficiali di diverso grado. E' possibile disporre i* 36 *ufficiali in fila per* 6 *in modo che su ogni riga e ogni colonna non si trovino due ufficiali dello stesso reggimento e dello stesso grado?*

OSSERVAZIONE 173

Il problema sembra apparentemente un quesito da giornale di enigmistica, ma in realtà è molto profondo e basta provare a risolverlo per accorgersi che ciò non può essere fatto senza l'uso di appropriati strumenti matematici:

la teoria dei *quadrati latini*.

Questa è utile per lo studio di molti problemi di combinatoria, tra cui il calcolo di $A_q(4,3)$, come vedremo.

Sia X un insieme finito con $n > 1$ elementi.

DEFINIZIONE 174

Una matrice $A = (a_{ij})$ di tipo $n \times n$ ad elementi in X prende il nome di *quadrato latino su X* se ogni riga e ogni colonna di A è una permutazione di X. L'intero n si chiama *ordine* del quadrato latino.

ESEMPIO 175

La tabella di addizione dell'anello Z_n degli interi modulo n è un quadrato latino d'ordine n.

DEFINIZIONE 176

Due quadrati latini $A = (a_{ij})$ e $B = (b_{ij})$ si dicono *ortogonali* se risulta

$$X \times X = \{(a_{ij}, b_{ij}) \quad : \quad i, j = 1, 2, .., n\},$$

cioè se, per ogni coppia (x, y) di elementi di X, esiste un'unica coppia di indici (i, j) tale che $a_{ij} = x$ e $b_{ij} = y$.

ESEMPI 177

La matrice

$$\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$$

è un quadrato latino su $X = \{1, 2\}$ e

$$A_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix}$$

sono tre quadrati latini su $X = \{1, 2, 3, 4\}$ a due a due ortogonali.

Quadrati latini ortogonali

Costruire quadrati latini a due a due ortogonali non è facile, nemmeno per ordini piccoli. Per esempio, il problema dei 36 ufficiali equivale a chiedersi se esistono due quadrati latini ortogonali d'ordine 6.

L. Euler non riuscì a risolverlo e, intuendo che forse non aveva soluzione, formulò una famosa congettura secondo la quale *non esistono due quadrati latini ortogonali di ordine n, per ogni* $n \equiv 2 (mod\ 4)$.

Solo nel 1900 *G.Tarry* provò che il problema dei 36 ufficiali non aveva soluzione.

La congettura, invece, si è rivelata falsa; infatti nel 1960 *R.C.Bose, E.T.Parker e E.T.Shrikhande* provarono che *gli unici interi* $n > 1$ *per cui non esistono due quadrati latini ortogonali d'ordine n sono* 2 *e* 6.

Quadrati latini simili

DEFINIZIONE 178

Due quadrati latini su X si dicono *simili* se si ottengono sostituendo ogni elemento del primo con il corrispondente del secondo in una fissata permutazione σ su X.

ESEMPIO 179

I quadrati latini $\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$ e $\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$ sono simili.

PROPOSIZIONE 180

La relazione di similitudine fra quadrati latini è di equivalenza. Inoltre, due quadrati latini rispettivamente simili a due quadrati latini ortogonali sono a loro volta ortogonali.

ESEMPIO 181

Lo studio dei quadrati latini può farsi a meno della relazione di similitudine. Questo significa che, quando abbiamo un insieme di quadrati latini mutuamente ortogonali, non è restrittivo supporre che abbiano le prime righe uguali.

PROPOSIZIONE 182

Per ogni intero $n > 1$, esistono al più $n - 1$ quadrati latini d'ordine n mutuamente ortogonali.

DIMOSTRAZIONE

Se abbiamo m quadrati latini d'ordine n mutualmente ortogonali, possiamo supporre che essi abbiano tutti lo stesso elemento a di posto $(1, 1)$. Allora, in forza dell'ortogonalità, gli elementi di posto $(2, 1)$ devono essere fra loro a due a due distinti e diversi da a. Ne segue che è $m \leq n - 1$, cioè l'asserto.

DEFINIZIONE 183

Un insieme di $n - 1$ quadrati latini d'ordine n e mutuamente ortogonali si chiama *sistema completo* di quadrati latini mutuamente ortogonali.

Nel caso $n = 4$, un sistema completo di quadrati latini mutuamente ortogonali è dato dall'esempio 177.

Ricordiamo che con $A_q(n,d)$ si denota il più grande intero M per cui esiste un $(n,M,d)-$codice $q-$ario.

PROPOSIZIONE 184

Per ogni intero $q > 1$, risulta

$$A_q(4,3) \leq q^2 \tag{25}$$

DIMOSTRAZIONE

Sia C un $(4,M,3)-$codice su un alfabeto F_q con q lettere. Se $\mathbf{a} = a_1a_2a_3a_4$ e $\mathbf{b} = b_1b_2b_3b_4$ sono parole distinte di C, risulta $(a_1,a_2) \neq (b_1,b_2)$, perché $d(C) = 3$. Ne segue che M non può superare q^2.

ESEMPIO 185

Per il $(4,9,3)-$codice ternario

0000	0112	0221
1011	1120	1202
2022	2101	2210

si raggiunge il massimo consentito dalla (25).

OSSERVAZIONE 186

La limitazione $A_q(4,3) \leq q^2$, per $q > 4$, migliora di molto la disuguaglianza di Hamming

$$A_q(4,3) \leq q^4/(4q-3).$$

OSSERVAZIONE 187

Un $(4, q^2, 3)-$codice C su F_q è necessariamente del tipo

$$C = \{(i, j, a_{ij}, b_{ij}) \ : \ (i,j) \in F_q^2\}. \tag{26}$$

La funzione $A_q(4,3)$

PROPOSIZIONE 188

Un codice C del tipo (26) ha distanza minima 3 se, e solo se, $A = [a_{ij}]$ e $B = [b_{ij}]$ sono due quadrati latini ortogonali.

DIMOSTRAZIONE

Basta osservare che valgono le seguenti equivalenze:

- Le q^2 coppie (i, a_{ij}) sono distinte e le q^2 coppie (j, a_{ij}) sono distinte $\Leftrightarrow$ A è un quadrato latino.
- Le q^2 coppie (i, b_{ij}) sono distinte e le q^2 coppie (j, b_{ij}) sono distinte $\Leftrightarrow$ B è un quadrato latino.
- Se A e B sono quadrati latini, le q^2 coppie (a_{ij}, b_{ij}) sono distinte $\Leftrightarrow$ A e B sono ortogonali.

COROLLARIO (Bose,Parker,Shrikhande,1960) 189

Per ogni intero $q \neq 2, 6$ risulta $A_q(4,3) = q^2$.

OSSERVAZIONE 190

Un $(n, q^2, n-1)-$codice C su un alfabeto con q lettere F_q è necessariamente del tipo

$$C = \{(i, j, a_{ij}^{(1)}, a_{ij}^{(2)}, \ldots, a_{ij}^{(n-2)}) \ : \ (i, j) \in F_q^2\}.$$

PROPOSIZIONE 191

L'esistenza di un $(n, q^2, n-1)-$ codice $q-$ario equivale a quella di un insieme di $n-2$ quadrati latini mutuamente ortogonali di ordine q.

DIMOSTRAZIONE

È lasciata come esercizio.

7. Equivalenza di codici

indice

DEFINIZIONE 192

Diciamo che due $(n, M) - codici$ sullo stesso alfabeto sono *equivalenti* se due matrici ad essi rispettivamente associate possono ottenersi l'una dall'altra mediante una successione finita di operazioni dei seguenti tipi:

(A) *scambio di due colonne (questa operazione equivale a scambiare tra loro in ogni parola del codice le lettere che si trovano in due posizioni fissate);*

(B) *applicazione di una permutazione dell'alfabeto F alle lettere che si trovano in una fissata colonna.*

Esempi di codici equivalenti

Si consideri il codice ternario

$$C_1 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 0 \\ 0 & 1 & 2 & 0 & 2 \\ 2 & 1 & 0 & 2 & 0 \end{bmatrix}$$

sull'alfabeto $F = \{0, 1, 2\}$. Il codice

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 2 & 1 & 1 & 2 & 0 \\ 1 & 0 & 0 & 2 & 2 \\ 1 & 2 & 2 & 0 & 0 \end{bmatrix}$$

è equivalente a C_1 perchè si ottiene da questo scambiando la prima colonna con la seconda e la terza con la quarta. Ancora, il codice

$$\begin{bmatrix} 1 & 0 & 2 & 0 & 1 \\ 1 & 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 2 \\ 2 & 1 & 1 & 2 & 0 \end{bmatrix}$$

è equivalente a C_1 perché si ottiene da questo applicando la permutazione ciclica $(0, 1, 2)$ alle lettere della terza colonna.

ESERCIZIO 193

Provare che i seguenti $(5,4)-$codici sull'alfabeto $F=\{0,1,2\}$

$$C_1=\begin{bmatrix}1&0&1&0&1\\1&2&2&1&0\\0&1&2&0&2\\2&1&0&2&0\end{bmatrix}, C_2,=\begin{bmatrix}2&0&1&2&0\\0&1&2&2&1\\1&1&0&1&0\\0&2&1&0&2\end{bmatrix}$$

sono equivalenti.

PROPOSIZIONE 194

Siano C_1 e C_2 due codici equivalenti. Allora, per ogni intero positivo t, il numero di coppie di parole di C_1 a distanza t è uguale al corrispondente numero in C_2.

Codici equivalenti

L'equivalenza tra codici è una relazione di equivalenza nella classe di tutti i codici.

Per questo motivo, lo studio dei codici verrà fatto a meno di equivalenze.

GENERALITÀ SUI CODICI LINEARI

1. Prime definizioni ed esempi

indice

DEFINIZIONE 195

Una struttura algebrica con due operazioni interne (*addizione e moltiplicazione*) $F = (F, +, \cdot)$ prende il nome di *corpo* se sono verificate le seguenti proprietà:

(1) F è un gruppo abeliano rispetto all'addizione;

(2) $F^* = F \setminus \{0\}$ è un gruppo rispetto alla moltiplicazione;

(3) la moltiplicazione in F è distributiva rispetto all'addizione, cioè

$$(a+b)c = ac + bc\,, \text{ per ogni } a, b, c \in F\,.$$

Sia $F = (F, +, \cdot)$ un corpo. I gruppi $(F, +)$ e $(F^*, \cdot)$ si chiamano, rispettivamente, *gruppo additivo* e *gruppo moltiplicativo* di F.

Come al solito, 0 (*zero*) e 1 (*unità*) denotano rispettivamente gli elementi neutri di $(F, +)$ e $(F^*, \cdot)$.

DEFINIZIONE 196

Il corpo F prende il nome di *campo* se la moltiplicazione è commutativa, cioè se il suo gruppo moltiplicativo è abeliano.

In un corpo si definiscono in modo usuale le nozioni di *sottocorpo*, *sottocampo*, *sottocorpo e sottocampo generato da un insieme di elementi*.

RISULTATO (Teorema di Wedderburn) 197

Ogni corpo finito è un campo.

Sottocampo fondamentale di un campo F

DEFINIZIONE 198

Si dice che F ha *caratteristica zero* se:

$$c \in N \ , \ ca = 0 \ \text{per ogni} \ a \in F \ \Rightarrow \ c = 0 \, .$$

Nel caso contrario, se p è il più piccolo intero positivo per cui $pa = 0$, per ogni $a \in F$, si dice che F ha *caratteristica p*. La caratteristica di F si denota con $char(F)$.

DEFINIZIONE 199

L'intersezione di tutti i sottocampi di F è, rispetto all'inclusione, il minimo sottocampo di F e coincide col sottocampo generato da 1. Tale sottocampo si chiama *sottocampo fondamentale* o *sottocampo primo* di F.

RISULTATO 200

Se $char(F) = p > 0$, allora p è un primo. Inoltre, il sottocampo fondamentale di F è isomorfo al campo razionale Q o al campo Z_p dei resti modulo p a seconda che $char(F) = 0$ o $char(F) = p > 0$, rispettivamente.

Estensioni

Nel seguito denoteremo con F un campo e con K un suo sottocampo. In queste ipotesi, si dice anche che F è un'*estensione* di K e si scrive F/K. Si ha:

- Ogni campo è estensione del proprio sottocampo fondamentale.
- F è uno spazio vettoriale su K la cui dimensione si chiama anche *grado* di F su K e si denota con $dim_K F$ o $[F : K]$.

DEFINIZIONE 201

Quando la dimensione di F su K è finita, si dice che F è un'*estensione di grado finito* di K, o che F/K è *di grado finito.*

ESEMPI 202

Il campo R dei numeri reali è un'estensione di grado infinito del campo Q dei razionali.

Nel campo $C = \{a + ib : a, b \in R,\ i^2 = -1\}$ dei numeri complessi, considerato come spazio vettoriale sui reali, l'insieme $\{1, i\}$ è una base. Ne segue che C è un'estensione finita di R di grado 2.

Campi di spezzamento di polinomi

RISULTATO 203

Sia $f \in K[x]$ un polinomio irriducibile su K. Allora esiste un'estensione F di K contenente una radice a di f.

DEFINIZIONE 204

Sia f un polinomio di grado $n > 0$ a coefficienti in un campo K. Un'estensione F di K si chiama *campo di spezzamento* di f su K se contiene n elementi $a_1, a_2, \ldots, a_n \in F$ (non necessariamente distinti) tali che:
(1) $f(x) = a(x - a_1)(x - a_2) \cdots (x - a_n)$ con $a \in K$;
(2) il sottocampo di F generato da K e $a_1, a_2, \ldots a_n$ coincide con F.

RISULTATO 205

Per ogni polinomio di grado $n > 0$ a coefficienti in un campo K esiste, unico a meno di isomorfismi, un campo di spezzamento su K.

ESEMPIO 206

Il polinomio $x^2 + 1$ è irriducibile sul campo reale. Il suo campo di spezzamento è il campo complesso, ove risulta $x^2 + 1 = (x - i)(x + i)$.

Denoteremo con F_q un campo finito d'ordine q e caratteristica p. Il sottocampo fondamentale di F_q è isomorfo a Z_p, il campo dei resti modulo l'intero primo p.

PROPOSIZIONE 207

Siano F_q un campo finito e $F_{q'}$ un suo sottocampo d'ordine q'. Allora
(i) *esiste un intero positivo h tale che $|F_q| = q = p^h$;*
(ii) *se $|F_{q'}| = p^{h'}$, h' divide h;*
(iii) *se h è primo, Z_p é l'unico sottocampo proprio di F_q.*

DIMOSTRAZIONE

F_q ha grado finito h su Z_p e, quindi, come spazio vettoriale su Z_p è isomorfo a Z_p^h, che contiene esattamente p^h elementi. Con analogo ragionamento si prova il resto del teorema.

PROPOSIZIONE 208

Denotati con $a_1, a_2, .., a_{q-1}$ gli elementi non nulli di F_q, risulta:

$$a^{q-1} = 1 \quad , \quad \text{per ogni } a \in F_q^*; \tag{27}$$

$$a^q = a \quad , \quad \text{per ogni } a \in F_q; \tag{28}$$

$$a_1 a_2 \cdots a_{q-1} = -1. \tag{29}$$

DIMOSTRAZIONE

La (27) è vera perché il gruppo moltiplicativo F_q^* è finito e ha ordine $q-1$. La (28) segue da (27) e assicura che il polinomio $x^q - x$ puó essere scritto nella forma

$$x^q - x = x(x - a_1)(x - a_2) \cdots (x - a_{q-1}); \tag{30}$$

cosí , uguagliando i coefficienti dei termini di primo grado, si ha

$$(-1)^{q-1} a_1 a_2 \cdots a_{q-1} = a_1 a_2 \cdots a_{q-1} = -1$$

e resta provata anche la (29).

ESERCIZIO 209

1. Provare che la somma di tutti gli elementi $0, a_1, a_2, .., a_{q-1}$ di un campo finito F_q d'ordine q maggiore di due è uguale a zero (si usi la relazione $x^q - x = x(x - a_1)(x - a_2) \cdots (x - a_{q-1})$).
2. Provare che un polinomio del tipo

$$(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_t),$$

con $\alpha_1, \alpha_2, ..., \alpha_t$ elementi a due a due distinti di F_q, è divisibile per $x^q - x$.

OSSERVAZIONE 210

In un campo finito non vale il principio di identità dei polinomi (due polinomi sono uguali se, e solo se, lo sono le loro funzioni polinomiali). La (28), infatti, mostra che il polinomio non nullo $x^q - x \in F_q[x]$ ha funzione polinomiale identicamente nulla.

PROPOSIZIONE 211

Ogni campo finito F_q d'ordine $q = p^h$ è campo di spezzamento del polinomio $x^q - x$ su Z_p. Di conseguenza campi finiti dello stesso ordine sono isomorfi.

DIMOSTRAZIONE

La prima parte segue dalla relazione

$$x^q - x = x(x - a_1)(x - a_2)\cdots(x - a_{q-1}), \quad a_j \in F_q; \qquad (31)$$

e dalla definizione di campo di spezzamento. La seconda parte segue dall'unicità del campo di spezzamento.

RISULTATO 212

Siano p un primo, h un intero positivo e $q = p^h$. Il campo di spezzamento del polinomio $x^q - x$ su Z_p è finito d'ordine q : un tale campo si chiama campo di Galois e si denota con $GF(q)$.

CONCLUSIONE 213

Per ogni primo p e per ogni intero positivo h, esiste un unico campo finito d'ordine $q = p^h$, a meno di isomorfismi.

RISULTATO 214

Per ogni divisore k di h esiste un unico sottocampo di F_q d'ordine p^k.

CONVENZIONE 215

D'ora in avanti porremo:

- q potenza di un primo p;
- $F = F_q$, campo finito con q elementi;
- $F^n = F_q^n = V(n, q)$ spazio vettoriale numerico di dimensione n sul campo F.

DEFINIZIONE 216

Un *codice lineare* è un sottospazio vettoriale di F^n.

ESEMPIO 217

Il codice *ASCII* e il codice *ASCII* esteso sono esempi di codici lineari su Z_2.

PROPOSIZIONE 218

Un codice lineare C di dimensione k è isomorfo, come spazio vettoriale, a F_q^k e, quindi, è $|C| = |F_q^k| = q^k$.

DEFINIZIONE 219

Un codice lineare C di dimensione k e distanza minima d si dice $[n, k, d]-$*codice*, o $[n, k]-$*codice*. Gli interi n, k e d si dicono *parametri di* C.

OSSERVAZIONE 220

Un $[n, k, d]-$codice è chiaramente un $(n, q^k, d) -$ *codice*.

CONVENZIONE 221

D'ora in avanti riterremo fissato un $[n, k, d]-$codice C e denoteremo sempre con $\mathbf{0}$ il vettore nullo (*parola nulla*).

DEFINIZIONE 222

Si chiama *peso* di una parola $\mathbf{a} \in F^n$, e si denota con $w(\mathbf{a})$, il numero delle componenti di $\mathbf{a}$ diverse da zero o, equivalentemente, la distanza di $\mathbf{a}$ dalla parola nulla:

$$w(\mathbf{a}) = d(\mathbf{a}, \mathbf{0})$$

Il minimo $w(C)$ dei pesi delle parole di C diverse da $\mathbf{0}$ si chiama *peso minimo* di C, cioè

$$w(C) := min\{w(\mathbf{a}) : \mathbf{a} \in C, \mathbf{a} \neq \mathbf{0}\}.$$

Quando non vi è possibilità di equivoci, scriveremo w in luogo di $w(C)$.

OSSERVAZIONE 223

Se due parole $\mathbf{a}$ e $\mathbf{b}$ di C hanno distanza h, allora la parola $\mathbf{a}-\mathbf{b}$, che è ancora in C, ha peso h : $d(\mathbf{a},\mathbf{b}) = d(\mathbf{a}-\mathbf{b},\mathbf{0}) = w(\mathbf{a}-\mathbf{b})$. Ne segue che in ogni $[n,k,d]-$codice risulta

$$d = w. \tag{32}$$

Questo è un primo vantaggio offerto dalla proprietà di linearità di un codice C: per valutare d basta calcolare i pesi delle $M-1 = q^k-1$ parole di C diverse da $\mathbf{0}$. In assenza di linearità, invece, per determinare d occorre calcolare $M(M-1)/2$ distanze e tale numero è dell'ordine di M^2.

OSSERVAZIONE 224

Un secondo e importante vantaggio di un codice lineare C è che esso può essere descritto completamente (e quindi implementato su una macchina) da una sua base.

DEFINIZIONE 225

Una matrice le cui righe costituiscono una base di C si chiama *matrice generatrice* di C.

OSSERVAZIONE 226

Se C ha parametri $[n, k, d]$, una sua matrice generatrice G è di tipo $k \times n$. In queste ipotesi C è il sottospazio generato dalle righe di G (*spazio delle righe di G*):

$$C = \{\mathbf{x}G : \mathbf{x} \in F_q^k\}.$$

ESEMPIO 227

Il codice $C = \{(0,0,0),(1,1,0),(1,0,1),(0,1,1)\}$ è un $[3,2,2]-$codice binario con matrice generatrice

$$G = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

e risulta

$$(0,0,0) = (0,0)G, \quad (1,1,0) = (1,1)G,$$
$$(1,0,1) = (0,1)G, \quad (0,1,1) = (1,0)G$$

ESEMPIO 228

Il codice di ripetizione $q-$ario di lunghezza n è un $[n,1,n]$-codice con matrice generatrice $G = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \end{bmatrix}$.

Esempio

Il *codice binario di Hamming*

$$H(3,2) = \begin{bmatrix} 1&1&0&1&0&0&0 \\ 1&0&1&0&0&1&0 \\ 0&0&0&1&1&1&0 \\ 0&0&1&1&0&0&1 \\ 0&1&1&0&1&0&0 \\ 1&0&0&0&1&0&1 \\ 0&1&0&0&0&1&1 \\ 0&0&0&0&0&0&0 \\ 1&1&1&1&1&1&1 \\ 0&0&1&0&1&1&1 \\ 0&1&0&1&1&0&1 \\ 1&1&1&0&0&0&1 \\ 1&1&0&0&1&1&0 \\ 1&0&0&1&0&1&1 \\ 0&1&1&1&0&1&0 \\ 1&0&1&1&1&0&0 \end{bmatrix} \begin{matrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \mathbf{a}_3 \\ \mathbf{a}_4 \\ \mathbf{a}_5 \\ \mathbf{a}_6 \\ \mathbf{a}_7 \\ \mathbf{0} \\ \mathbf{1} \\ \mathbf{b}_1 \\ \mathbf{b}_2 \\ \mathbf{b}_3 \\ \mathbf{b}_4 \\ \mathbf{b}_5 \\ \mathbf{b}_6 \\ \mathbf{b}_7 \end{matrix}$$

è un $[7,4,3]-$ codice lineare su Z_2.
Una sua matrice generatrice è

$$G = \begin{bmatrix} 1&1&1&1&1&1&1 \\ 1&0&0&0&1&0&1 \\ 1&1&1&0&0&0&1 \\ 0&1&0&0&0&1&1 \end{bmatrix}.$$

Il codice binario di Golay

La matrice

$$G_{23} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0
\end{bmatrix}$$

è la matrice generatrice di un $[23, 12]$-codice binario, noto come *codice binario di Golay*, che si denota con $\mathcal{G}_{23}$.

OSSERVAZIONE 229

Nel seguito proveremo che il peso minimo del $[23, 12]$-codice binario $\mathcal{G}_{23}$ è 7 e, di conseguenza, tale codice corregge 3 errori ed è perfetto:

$$2^{12}\left[\binom{23}{0}+\binom{23}{1}+\binom{23}{2}+\binom{23}{3}\right]=$$

$$2^{12}\left[1+23+11\cdot 23+7\cdot 11\cdot 23\right]=$$

$$=2^{12}\,2048=2^{12}\,2^{11}=2^{23}.$$

Marcel J.E.Golay

https://en.wikipedia.org/wiki/Marcel_J._E._Golay

03.05.1902 (Neuchâtel, Svizzera)
27.04.1989

Equivalenza di codici lineari

OSSERVAZIONE 230

L'applicazione di una permutazione delle lettere che si trovano in una fissata posizione di un codice lineare C [operazione di tipo (B)] non conserva la linearità. Per esempio, i codici binari $\{00, 11\}$ e $\{10, 01\}$ sono equivalenti e dei due solo il primo è lineare. In altre parole, un codice equivalente ad un codice lineare non è necessariamente lineare. Per i codici lineari serve una nozione meno generale di equivalenza!

DEFINIZIONE 231

Due codici lineari su F_q si dicono *linearmente equivalenti* se due matrici ad essi rispettivamente associate si ottengono l'una dall'altra mediante una successione finita di operazioni dei seguenti tipi (che conservano la linearità):

(A) *scambio di due colonne;*

(B') *moltiplicazione degli elementi di una fissata colonna per uno scalare non nullo.*

Equivalenza di codici lineari

CONVENZIONE 232

Nel seguito, poiché considereremo esclusivamente codici lineari, diremo che due tali codici sono *equivalenti* quando sono linearmente equivalenti.

PROPOSIZIONE 233

Due matrici G e G' su F generano codici lineari equivalenti se, e soltanto se, si ottengono l'una dall'altra mediante un numero finito di operazioni elementari dei tipi seguenti:
(R1) *scambio di due righe,*
(R2) *moltiplicazione di una riga per uno scalare non nullo,*
(R3) *sostituzione di una riga con la somma di quest'ultima e di un'altra riga,*
(C1) *scambio di due colonne,*
(C2) *moltiplicazione di una colonna per uno scalare non nullo.*

PROPOSIZIONE 234

Una matrice generatrice G di un $[n, k, d]-$codice C, mediante un numero finito di operazioni di tipo R1, R2, R3, C1, C2 può sempre trasformarsi nella forma (detta *forma standard* di G)

$$[I_k, A], \tag{33}$$

ove I_k è la matrice identità d'ordine k e A una matrice di tipo $k \times (n-k)$. Ne segue che ogni $[n, k, d]-$codice è $k-$sistematico.

OSSERVAZIONE 235

Nelle ipotesi della precedente proposizione, il codice generato dalle righe della matrice (33) è equivalente, ma non necessariamente uguale, a C.
Per esempio $C_1 = \{(0,0),(1,0)\}$ e $C_2 = \{(0,0),(0,1)\}$ sono codici lineari binari equivalenti e le loro uniche matrici generatrici sono rispettivamente $G_1 = [1\ 0]$ (che è in forma standard) e $G_2 = [0\ 1]$ (che non è in forma standard).

DEFINIZIONE 236

Il *prodotto scalare* (standard) di due vettori $\mathbf{a}$, $\mathbf{b}$ di $V(n, q)$ è definito da

$$\mathbf{ab} = (a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) =$$

$$a_1 b_1 + a_2 b_2 + \cdots + a_n b_n.$$

I vettori $\mathbf{a}, \mathbf{b}$ si dicono *ortogonali* se risulta $\mathbf{ab} = 0$.

PROPOSIZIONE 237

Per ogni $\mathbf{a}, \mathbf{b}, \mathbf{c} \in V(n, q)$ e $\lambda, \mu \in F$, si ha:

$$\mathbf{ab} = \mathbf{ba} \ , \ \ (\lambda\mathbf{a} + \mu\mathbf{b})\mathbf{c} = \lambda(\mathbf{ac}) + \mu(\mathbf{bc}) \qquad (34)$$

PROPOSIZIONE 238

Per $A \subseteq V(n, q)$,

$$A^{\perp} = \{\mathbf{x} \in V(n, q) \ : \ \mathbf{xa} = 0 \, , \ \textit{per ogni} \ \mathbf{a} \in A\}$$

è un sottospazio vettoriale di $V(n, q)$ (il *sottospazio ortogonale* ad A).

DIMOSTRAZIONE

Per ogni $\mathbf{x}, \mathbf{y} \in A^{\perp} e \ \lambda, \mu \in F_q$, risulta

$$(\lambda\mathbf{x} + \mu\mathbf{y})\mathbf{a} = \lambda(\mathbf{xa}) + \mu(\mathbf{ya}) = 0$$

e, quindi, $(\lambda\mathbf{x} + \mu\mathbf{y}) \in A^{\perp}$.

PROPOSIZIONE 239

Per ogni sottospazio vettoriale W di $V(n,q)$, risulta

$$dim(W) + dim(W^{\perp}) = n \tag{35}$$

DIMOSTRAZIONE

Se W è un sottospazio di dimensione k di $V(n,q)$ e $B = \{\mathbf{g}_i = (g_{i1}, g_{i2}, ..., g_{in}), i = 1, 2, ..., k\}$, una sua base, risulta $W^{\perp} = B^{\perp}$. Allora $W^{\perp}$ è il sottospazio costituito dai vettori $\mathbf{x} = (x_1, x_2, ..., x_n)$ che sono soluzione del sistema $\mathbf{x}(g_{ij})^t = \mathbf{0}$, cioè

$$\begin{cases} g_{11}x_1 + g_{12}x_2 + \cdots + g_{1n}x_n = 0 \\ g_{21}x_1 + g_{22}x_2 + \cdots + g_{2n}x_n = 0 \\ \vdots \\ g_{k1}x_1 + g_{k2}x_2 + \cdots + g_{kn}x_n = 0 \end{cases}.$$

Poiché la matrice (g_{ij}) ha rango k, lo spazio delle soluzioni del sistema, cioè $W^{\perp}$, ha dimensione $n - k$ e, quindi, $dim(W) + dim(W^{\perp}) = k + n - k = n$.

OSSERVAZIONE 240

Se C è un $[n,k]-$codice, il sottospazio $C^{\perp}$ ortogonale a C è un codice con parametri $[n,n-k]$ e risulta $C^{\perp\perp}=C$. Detta, inoltre, G una matrice generatrice di C, risulta

$$\mathbf{a}\in C^{\perp} \quad \Leftrightarrow \quad \mathbf{a}G^{t}=\mathbf{0}\ .$$

DEFINIZIONE 241

L'$[n,n-k]-$codice $C^{\perp}$ si chiama *codice duale*, o *ortogonale*, di C e una sua matrice generatrice H prende il nome di *matrice di controllo* (di parità) di C.

PROPOSIZIONE 242

Una matrice H è di controllo per C se, e solo se, ha le seguenti proprietà:

$$\begin{cases} GH^t = 0, \\ \\ C = \{\mathbf{x} \in V(n,q) \ : \ \mathbf{x}H^t = 0\}. \end{cases} \tag{36}$$

Se supponiamo $G = [I_k, A]$ in forma standard, allora

$$H = [-A^t \ , \ I_{n-k}]$$

è una matrice controllo di parità di C.

DIMOSTRAZIONE

La prima parte è evidente; per la seconda basta osservare che è $$GH^t = [I_k, A][-A^t \ , \ I_{n-k}]^t = I_k(-A) + AI_{n-k} = 0.$$

ESEMPIO 243

Per il $[3, 2, 2]-$codice binario

$$C = \{(0,0,0), (1,1,0), (1,0,1), (0,1,1)\}$$

si ha:

$$G = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad , \quad H = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}.$$

ESEMPIO 244

Il codice ortogonale all'$[n, 1, n]-$codice di ripetizione $q-$ario è l'$[n, n-1, 2]_q-$codice formato da tutte e sole le parole $\mathbf{x} \in F_q^n$ tali che

$$x_1 + x_2 + \cdots + x_n = 0.$$

ESEMPIO 245

Per il $[5, 2, 3]-$codice binario

$$C = \{(0,0,0,0,0), (1,1,0,1,1), (1,0,1,1,0), (0,1,1,0,1)\}$$

si ha:

$$G = [I_2, A] = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix},$$

$$H = [-A^t, I_3] = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Codici autoortogonali e autoduali

DEFINIZIONE 246

Quando C è contenuto in $C^{\perp}$, diciamo che è un codice *autoortogonale*. Se un codice autoortogonale C coincide con $C^{\perp}$, diciamo che C è *autoduale*.

PROPOSIZIONE 247

Per C autoortogonale si ha $n = dim(C) + dim(C^{\perp}) \geq 2dim(C)$, e

$$\begin{cases} C \text{ autoortogonale} & \Rightarrow \quad dim(C) \leq \frac{n}{2}, \\ C \text{ autoduale} & \Rightarrow \quad dim(C) = \frac{n}{2}. \end{cases} \tag{37}$$

DIMOSTRAZIONE

Basta osservare che, essendo $C \subseteq C^{\perp}$. risulta $dim(C^{\perp}) \geq dim(C)$.

OSSERVAZIONE 248

In un codice autoduale ogni matrice generatrice è anche di controllo di parità e viceversa. In un codice autoortogonale binario ogni parola del codice ha peso pari (*codice pari*).

DEFINIZIONE 249

Per ogni parola $\mathbf{a} = (a_1, a_2, ..., a_n)$ su F_q, diciamo *controllo di parità* di $\mathbf{a}$ l'opposto della somma delle sue componenti, cioè

$$\overline{a} = -(a_1 + a_2 + \cdots + a_n).$$

Fissato allora l' $[n, k, d]-$codice C, l' $[n+1, k]-$codice $\overline{C}$ definito da

$$\overline{C} = \{\mathbf{a}' = (a_1, a_2, ..., a_n, \overline{a}) \ : \ \mathbf{a} \in C\},$$

si chiama *codice esteso* di C (provare per esercizio che questa definizione è corretta, cioè che $\overline{C}$ è un sottospazio vettoriale di F_q^{n+1} della stessa dimensione di C).

OSSERVAZIONE 250

Se un codice binario C ha peso minimo d, allora $\overline{C}$ ha peso minimo d o $d+1$ a seconda che d sia rispettivamente pari o dispari. Ovviamente ha senso considerare il codice esteso $\overline{C}$ solo quando C contiene qualche parola con controllo di parità non nullo. E', quindi, inutile considerare il codice esteso di $\overline{C}$.

OSSERVAZIONE 251

Aggiungendo il controllo di parità ad ogni riga di una matrice generatrice di un codice C si ottiene una matrice generatrice del codice esteso $\overline{C}$.

ESERCIZIO 252

Provare che, se C ha matrice controllo di parità H, allora

$$\overline{H} = \begin{bmatrix} & & & 0 \\ & H & & \vdots \\ & & & 0 \\ 1 & 1 & \cdots & 1 \end{bmatrix}$$

è una matrice controllo di parità per $\overline{C}$.

OSSERVAZIONE 253

Se a tutte le parole di un codice C si aggiunge il controllo di parità in una qualunque prefissata posizione, si ottiene un codice equivalente al codice esteso $\overline{C}$.

Il codice esteso $\overline{C}$ del $[5,2,3]-$codice binario

$$C = \{(0,0,0,0,0),(1,1,0,1,1),(1,0,1,1,0),(0,1,1,0,1)\}$$

è

$$\overline{C} = \{(0,0,0,0,0,0),(1,1,0,1,1,0),(1,0,1,1,0,1),(0,1,1,0,1,1)\}.$$

Le matrici

$$\overline{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}, \quad \overline{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

sono rispettivamente una matrice generatrice e una di controllo di $\overline{C}$.
I codici

$$\{(0,0,0,0,0,0),(0,1,1,0,1,1),(1,1,0,1,1,0),(1,0,1,1,0,1)\}$$

$$\{(0,0,0,0,0,0),(1,1,0,0,1,1),(1,0,1,1,1,0),(0,1,1,1,0,1)\}$$

sono codici equivalenti a $\overline{C}$.

Il codice binario di Golay esteso

Il $[24, 12]$-codice esteso di $\mathcal{G}_{23}$ si chiama *codice binario di Golay esteso* e si denota con $\mathcal{G}_{24}$. Una sua matrice generatrice è data da

$$G_{24} = \left[\begin{array}{c|cccccccccccc} & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ I_{12} & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right].$$

OSSERVAZIONE 254

In seguito proveremo che $\mathcal{G}_{24}$ è autoduale, ha distanza minima 8 e, quindi, corregge 3 errori.

OSSERVAZIONE 255

Questo codice è stato usato dalla *NASA* nel 1979 e nel 1981 per trasmettere sulla terra fotografie a colori ad alta risoluzione ($2^{12} = 4096$ sfumature di colori) di Giove e Saturno dalle capsule spaziali *Voyager 1* e *Voyager 2*, rispettivamente.

Le sfumature di colore erano rappresentate dalle parole binarie di lunghezza 12 ed erano codificate con le parole di lungheza 24 di $\mathcal{G}_{24}$.

Foto di Giove trasmessa dallo spazio col codice $\mathcal{G}_{24}$

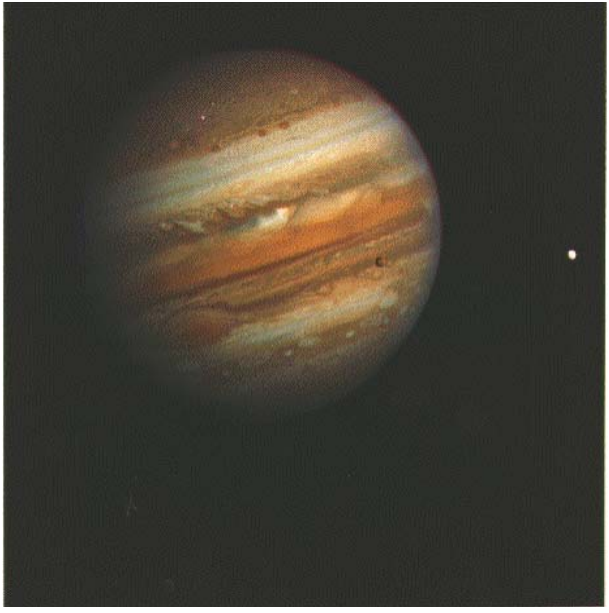
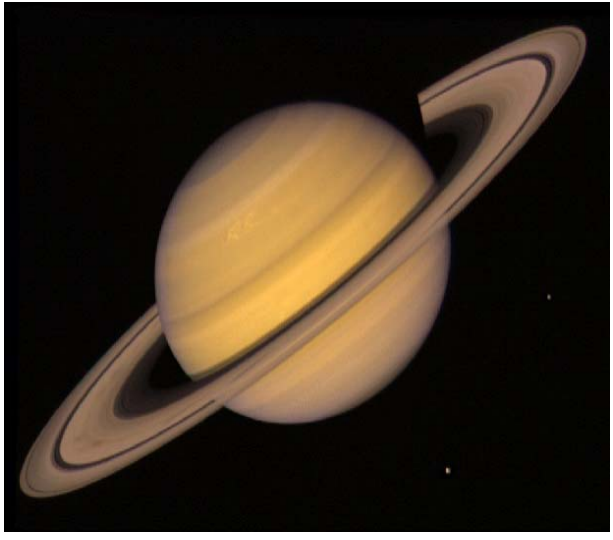


Foto di Saturno trasmessa dallo spazio col codice $\mathcal{G}_{24}$



2. Codifica e decodifica di un codice lineare

indice

DEFINIZIONE 256

Sia C un $[n,k]-$codice su F_q. Per ogni $\mathbf{u} \in F_q^n$, l'insieme

$$\mathbf{u} + C = \{\mathbf{u} + \mathbf{v}\,,\ \mathbf{v} \in C\}$$

prende il nome di laterale di C relativo a $\mathbf{u}$ (coset).

Una parola di peso minimo in $\mathbf{u} + C$ prende il nome di direttrice del laterale $\mathbf{u} + C$ (coset leader)

PROPOSIZIONE 257

In F_q^n, la relazione $\mathbf{u} \sim_L \mathbf{v}$ se, e solo se, $\mathbf{u} - \mathbf{v} \in C$ è di equivalenza. Inoltre, due vettori $\mathbf{v}, \mathbf{w} \in F_q^n$ appartengono ad uno stesso laterale di C se, e solo se, $\mathbf{v} - \mathbf{w}$ è una parola di C. Ne segue che la classe di equivalenza rispetto a $\sim_L$ di un vettore $\mathbf{u}$ coincide con il laterale $\mathbf{u} + C$.

DIMOSTRAZIONE

Il codice C, in quanto sottospazio vettoriale di F_q^n, contiene il vettore nullo e l'opposto di ogni suo elemento, e da qui seguono le proprietà riflessiva e simmetrica. Ora, se $\mathbf{u} - \mathbf{v} \in C$ e $\mathbf{v} - \mathbf{w} \in C$, allora

$$C \ni (\mathbf{u} - \mathbf{v}) + (\mathbf{v} - \mathbf{w}) = \mathbf{u} - \mathbf{w},$$

cioè la proprietà transitiva.
Se $\mathbf{v}, \mathbf{w} \in \mathbf{u} + C$, cioè $\mathbf{v} = \mathbf{u} + \mathbf{a}$, $\mathbf{w} = \mathbf{u} + \mathbf{b}$ con $\mathbf{a}, \mathbf{b} \in C$, allora $\mathbf{v} - \mathbf{w} = (\mathbf{u} + \mathbf{a}) - (\mathbf{u} + \mathbf{b}) = \mathbf{a} - \mathbf{b} \in C$.
Se $\mathbf{v} - \mathbf{w} = \mathbf{a} \in C$, allora da $\mathbf{v} = \mathbf{w} + \mathbf{a}$ e $\mathbf{w} = \mathbf{w} + \mathbf{0}$ segue $\mathbf{v}, \mathbf{w} \in \mathbf{w} + C$.

Sia C un $[n, k]-$codice su F_q. Dalla definizione di laterale e dall'ultima proposizione segue che:

- $\mathbf{u} \in \mathbf{u} + C$, per ogni $\mathbf{u} \in F_q^n$.
- $|\mathbf{u} + C| = |C| = q^k$, per ogni $\mathbf{u} \in F_q^n$.
- I laterali di C sono una partizione di F_q^n e, quindi, sono a due a due disgiunti.
- Il numero dei laterali distinti di C è q^{n-k}.

- Assumiamo di dover trasmettere q^k messaggi da un unsieme $\mathcal{M}$, che possiamo identificare con l'insieme dei vettori di F_q^k. Allora, per la codifica di canale, possiamo supporre di utilizzare un $[n,k]-$codice C su F_q; risulta, infatti,

$$\mid C \mid = \mid F_q^k \mid = q^k.$$

- Se G è una matrice generatrice di C, della quale denotiamo con $\mathbf{g}_i$ i vettori riga, scegliamo come *funzione di codifica* l'applicazione

$$\mathbf{a} = (a_1, a_2, ..., a_k) \in F_q^k$$

$$\downarrow$$

$$a_1\mathbf{g}_1 + a_2\mathbf{g}_2 + \cdots + a_k\mathbf{g}_k = \mathbf{a}G \in C,$$

che è un isomorfismo di spazi vettoriali.

OSSERVAZIONE 258

L'*algoritmo di codifica* (di canale) è il prodotto (righe per colonne) di vettori numerici di lunghezza k per la matrice G.

Se $\mathcal{M} = Z_2^4$ e $C = Ham(3,2)$ è il $[7,4,3]-$ codice binario di Hamming, abbiamo

$$H(3,2) = \begin{bmatrix} 1&1&0&1&0&0&0 \\ 1&0&1&0&0&1&0 \\ 0&0&0&1&1&1&0 \\ 0&0&1&1&0&0&1 \\ 0&1&1&0&1&0&0 \\ 1&0&0&0&1&0&1 \\ 0&1&0&0&0&1&1 \\ 0&0&0&0&0&0&0 \\ 1&1&1&1&1&1&1 \\ 0&0&1&0&1&1&1 \\ 0&1&0&1&1&0&1 \\ 1&1&1&0&0&0&1 \\ 1&1&0&0&1&1&0 \\ 1&0&0&1&0&1&1 \\ 0&1&1&1&0&1&0 \\ 1&0&1&1&1&0&0 \end{bmatrix} \begin{matrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \mathbf{a}_3 \\ \mathbf{a}_4 \\ \mathbf{a}_5 \\ \mathbf{a}_6 \\ \mathbf{a}_7 \\ \mathbf{0} \\ \mathbf{1} \\ \mathbf{b}_1 \\ \mathbf{b}_2 \\ \mathbf{b}_3 \\ \mathbf{b}_4 \\ \mathbf{b}_5 \\ \mathbf{b}_6 \\ \mathbf{b}_7 \end{matrix},$$

$$G = \begin{bmatrix} 1&1&1&1&1&1&1 \\ 1&0&0&0&1&0&1 \\ 1&1&1&0&0&0&1 \\ 0&1&0&0&0&1&1 \end{bmatrix}.$$

e l'algoritmo di codifica $\mathbf{x} = \mathbf{a}G$ è:

$$\mathbf{a} = (a_1, a_2, a_3, a_4) \in Z_2^4$$

$$\downarrow$$

$$(a_1 + a_2 + a_3, a_1 + a_3 + a_4, a_1 + a_3, a_1, a_1 + a_2, a_1 + a_4, a_1 + a_2 + a_3 + a_4) \in C.$$

ESEMPIO 259

Se $\mathcal{M} = \{(0,0),(1,0),(0,1),(1,1)\}$
e $C = \{(0,0,0,0),(1,0,1,1),(0,1,0,1),(1,1,1,0)\}$, abbiamo

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

In questo caso, l'algoritmo di codifica $\mathbf{x} = \mathbf{a}G$ opera nel seguente modo:

$$\begin{array}{ccccc} \mathcal{M} & & \mathbf{a}G & & C \\ 00 & \to & (0,0)G & \to & 0000 \\ 10 & \to & (1,0)G & \to & 1011 \\ 01 & \to & (0,1)G & \to & 0101 \\ 11 & \to & (1,1)G & \to & 1110 \end{array}$$

OSSERVAZIONE 260

Quando $G = [I_k, A]$ è data in forma standard, le prime k lettere di $\mathbf{a}G$ coincidono ordinatamente con le componenti di $\mathbf{a}$; rappresentano cioè il messaggio, mentre le rimanenti $n - k$ sono le lettere di controllo (ridondanza).

ESEMPIO 261

Sia $\mathcal{M} = Z_2^4$ e consideriamo una matrice generatrice in forma standard del codice $Ham(3,2)$:

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

In questo caso, l'algoritmo di codifica $\mathbf{x} = \mathbf{a}G$ opera nel seguente modo:

$$\mathbf{a} = (a_1, a_2, a_3, a_4) \in Z_2^4$$

$$\downarrow$$

$$\mathbf{a}G = (a_1, a_2, a_3, a_4, a_1 + a_2 + a_4, a_1 + a_3 + a_4, a_2 + a_3 + a_4) \in C.$$

CONVENZIONE 262

Nel seguito, assegnati una parola $\mathbf{a} \in F_q^k$ e un $[n, k]$codice C $e-$correttore, supporremo che:

- $\mathbf{x} = \mathbf{a}G$ è la parola di C con la quale si codifica il messaggio $\mathbf{a} \in F_q^k$;
- la parola $\mathbf{x}$ è trasmessa e eventualmente ricevuta in errore: il decodificatore riceve una parola $\mathbf{y}$ non necessariamente uguale a $\mathbf{x}$;
- il numero di errori commessi su $\mathbf{x}$ non supera e, cioè $d(\mathbf{x}, \mathbf{y}) \leq e$.

PROBLEMA 263

Nelle nostre ipotesi, se $\mathbf{y} \notin C$, il decodificatore deve risalire in modo automatico a $\mathbf{x}$ con una decodifica di minima distanza. Serve, quindi, un algoritmo di decodifica che permetta di trovare una parola $\mathbf{z}$ di C a distanza minima da $\mathbf{y}$. Ricordiamo che, essendo C $e-$correttore e $d(\mathbf{x}, \mathbf{y}) \leq e$, risulterà

$$\mathbf{z} = \mathbf{x}.$$

Sia C un $[n, k]-$codice lineare $e-$correttore su F_q e si distribuiscano tutte le parole di F_q^n in una tabella (matrice) $\Sigma = (\sigma_{ij})$ con q^{n-k} righe e q^k colonne in modo che siano soddisfatte le seguenti proprietà:

(i) *la prima riga contiene tutte le parole di C ed è* $\sigma_{11} = \mathbf{0}$;

(ii) *per ogni indice di riga* i, *la parola* $\mathbf{a}_i = \sigma_{i1}$ *è di peso minimo rispetto a quelle contenute nella riga scelta e nelle righe successive;*

(iii) *per ogni coppia* (i, j) *di indici è* $\sigma_{ij} = \mathbf{a}_i + \sigma_{1j}$.

OSSERVAZIONE 264

È chiaro che la riga $i-$esima di Σ, per ogni indice i, contiene tutte le parole del laterale $\mathbf{a}_i + C$ di C. Inoltre, ogni laterale di C ha le sue parole distribuite su una riga di Σ. Osserviamo che la parola di un laterale di C che occupa la prima posizione nella corrispondente riga di Σ è una *direttrice* del laterale stesso.

PROPOSIZIONE 265

Σ è una tabella standard di C; risulta cioè

$$d(\sigma_{ij}, \sigma_{1j}) \leq d(\sigma_{ij}, \sigma_{1t}),$$

per ogni $t \neq j$.

DIMOSTRAZIONE

La prima riga di Σ contiene tutti e soli gli elementi del codice C e:

$$\sigma_{ij} = \mathbf{a}_i + \sigma_{1j},\ \sigma_{1j} - \sigma_{1t} \in C \ \Rightarrow\ w(\mathbf{a}_i) \leq w\left(\mathbf{a}_i + (\sigma_{1j} - \sigma_{1t})\right).$$

Pertanto risulta:

$$d(\sigma_{ij}, \sigma_{1j}) = w(\sigma_{ij} - \sigma_{1j}) = w(\mathbf{a}_i) \leq w\left(\mathbf{a}_i + (\sigma_{1j} - \sigma_{1t})\right) =$$

$$w\left((\mathbf{a}_i + \sigma_{1j}) - \sigma_{1t}\right) = w(\sigma_{ij} - \sigma_{1t}) = d(\sigma_{ij}, \sigma_{1t})$$

Algoritmo per la costruzione della tabella standard Σ

primo passo: distribuire le parole di C sulla prima riga di Σ con l'unica condizione $\sigma_{11} = \mathbf{0}$;

secondo passo: scegliere una parola $\mathbf{a}_2$ di peso minimo in $F_q^n \setminus C$ e porre $\sigma_{21} = \mathbf{a}_2$;

terzo passo: distribuire sulla seconda riga di Σ le parole di $\mathbf{a}_2 + C$ in modo che sia $\sigma_{2j} = \mathbf{a}_2 + \sigma_{1j}$;

quarto passo: scegliere una parola $\mathbf{a}_3$ di peso minimo in $F_q^n \setminus \{C \cup (\mathbf{a}_2 + C)\}$ e porre $\sigma_{31} = \mathbf{a}_3$;

quinto passo: distribuire sulla terza riga di Σ le parole di $\mathbf{a}_3 + C$ in modo che sia $\sigma_{3j} = \mathbf{a}_3 + \sigma_{1j}$;

..... continuare in questo modo fino all'esaurimento delle parole di F_q^n.

CONVENZIONE 266 Nel seguito, quando parleremo di tabella standard di un codice lineare intenderemo sempre che la tabella è stata costruita utilizzando l'algoritmo appena descritto.

ESEMPIO 267

Il $[4, 2]-$codice binario

$$C = \{(0,0,0,0), (1,0,1,1), (0,1,0,1), (1,1,1,0)\}$$

ha la seguente tabella standard

$$\Sigma = \begin{matrix} 0000 & 1011 & 0101 & 1110 \\ 1000 & 0011 & 1101 & 0110 \\ 0100 & 1111 & 0001 & 1010 \\ 0010 & 1001 & 0111 & 1100 \end{matrix}.$$

OSSERVAZIONE 268

Il codice C, avendo peso minimo 2, non corregge alcun errore. Ciò, per esempio, si riflette sul fatto che esistono parole come 0100 aventi la stessa distanza 1 da due parole $0000, 0101$ di C.

ESEMPIO 269

Il $[5,2]-$codice $C = \{(0,0,0,0,0),(1,0,1,1,0),(0,1,0,1,1),(1,1,1,0,1)\}$ ha la seguente tabella standard

$$\Sigma = \begin{array}{cccc} 00000 & 10110 & 01011 & 11101 \\ 10000 & 00110 & 11011 & 01101 \\ 01000 & 11110 & 00011 & 10101 \\ 00100 & 10010 & 01111 & 11001 \\ 00010 & 10100 & 01001 & 11111 \\ 00001 & 10111 & 01010 & 11100 \\ 10001 & 00111 & 10100 & 01100 \\ 11000 & 01110 & 10011 & 00101 \end{array}.$$

OSSERVAZIONE 270

Il codice C, avendo peso minimo 3, è $1-$correttore. Allora le sfere di centro le parole di C e raggio 1 sono a due a due disgiunte.

Decodifica con tabella: $\mathbf{x}$ = parola trasmessa, $\mathbf{y}$ = parola ricevuta

Sia assegnata una tabella standard di C.

SCHEMA DI DECODIFICA 271

Se i è l'indice della riga della tabella cui $\mathbf{y}$ appartiene e $\mathbf{a}_i$ la direttrice di tale riga, $\mathbf{y}$ si decodifica come $\mathbf{z} = \mathbf{y} - \mathbf{a}_i$.

OSSERVAZIONE 272

Poiché

$$d(\mathbf{y}, \mathbf{z}) = w(\mathbf{y} - \mathbf{z}) = w(\mathbf{a}_i)$$

è (per costruzione) la più piccola distanza $d(\mathbf{y}, \mathbf{a})$, al variare di $\mathbf{a} \in C$, siamo sicuri di aver usato uno schema di decodifica di minima distanza.

ALGORITMO DI DECODIFICA 273

primo passo: scorrere la tabella standard, iniziando dal primo elemento della prima riga e continuando in successione, fino a trovare la parola ricevuta $\mathbf{y}$;

secondo passo: decodificare $\mathbf{y}$ come la prima parola $\mathbf{z}$ della colonna della tabella cui $\mathbf{y}$ appartiene: $\mathbf{z} = \mathbf{y} - \mathbf{a}_i$, se $\mathbf{y}$ è sulla riga $i-$esima.

OSSERVAZIONE 274

Il buon esito dello schema di decodifica descritto si fonda sostanzialmente su due fatti:
(1) *l'errore* $\mathbf{y} - \mathbf{x}$, *che il decodificatore non conosce e deve scoprire, e la parola* **y** *ricevuta sono nello stesso laterale di* C;
(2) *la "speranza" che durante la trasmissione non si siano verificati "troppi" errori; cioè il peso di* $\mathbf{y} - \mathbf{x}$ *sia "abbastanza piccolo" in modo che* $\mathbf{y} - \mathbf{x}$ *abbia buona probabilità di coincidere con la direttrice del laterale* $\mathbf{y} + C$.

OSSERVAZIONE 275

Per decodificare **y** come

$$\mathbf{z} = \mathbf{y} - \mathbf{a}_i$$

basta sapere che **y** è sulla riga $i-$esima della tabella standard. La conoscenza della colonna cui **y** appartiene è inessenziale. L'algoritmo che usiamo, però, determina il posto esatto di **y** nella tabella!
Cerchiamo un algoritmo che ci restituisca soltanto la riga cui **y** *appartiene!*

DEFINIZIONE 276

Sia C un $[n,k]-$codice con matrice controllo di parità H. Per ogni vettore $\mathbf{a} \in V(n,q)$, diciamo *sindrome* di $\mathbf{a}$ il vettore $S(\mathbf{a}) \in V(n-k,q)$ definito da $S(\mathbf{a}) = \mathbf{a}H^t$.

PROPOSIZIONE 277

Se C è un $[n,k]-$codice, risulta $\mathbf{a} \in C \Leftrightarrow S(\mathbf{a}) = \mathbf{0}$. Inoltre, due vettori $\mathbf{a}, \mathbf{b} \in V(n,q)$ hanno la stessa sindrome se, e soltanto se, appartengono ad uno stesso laterale di C in $V(n,q)$. Ne segue che le sindromi sono in corrispondenza biunivoca con i laterali di C in $V(n,q)$.

DIMOSTRAZIONE

La prima parte è ovvia. Per la seconda, detti $\mathbf{a}$ e $\mathbf{b}$ due vettori di $V(n,q)$, risulta

$$\mathbf{a} + C = \mathbf{b} + C \Leftrightarrow \mathbf{b} - \mathbf{a} \in C \Leftrightarrow (\mathbf{b} - \mathbf{a})H^t = \mathbf{0} \Leftrightarrow$$
$$\mathbf{b}H^t - \mathbf{a}H^t = \mathbf{0} \Leftrightarrow \mathbf{a}H^t = \mathbf{b}H^t \Leftrightarrow S(\mathbf{a}) = S(\mathbf{b}).$$

Decodifica a sindromi: **y** = parola ricevuta

SCHEMA DI DECODIFICA A SINDROMI 278

(1) Si estende una tabella standard di C aggiungendo la colonna delle sindromi (elementi di una stessa riga hanno uguale sindrome);

(2) si calcola la sindrome $S(\mathbf{y})$ di $\mathbf{y}$ e, scorrendo la colonna delle sindromi, si trova l'indice i della riga cui $S(\mathbf{y})$ e $\mathbf{y}$ appartengono;

(3) y si decodifica come $\mathbf{z} = \mathbf{y} - \mathbf{a}_i$.

OSSERVAZIONE 279

Questo schema di decodifica necessita di una matrice M (*tabella per decodifica a sindromi*) con due sole colonne, la prima delle quali coincida con la prima colonna di una tabella standard Σ di C, la seconda con la colonna delle sindromi di Σ.

Decodifica a sindromi: **y** = parola ricevuta

ALGORITMO DI DECODIFICA A SINDROMI 280

Siano H una matrice controllo di parità di C e M una tabella per decodifica a sindromi

primo passo: *calcolare la sindrome $S(\mathbf{y}) = \mathbf{y}H^t$ della parola ricevuta* $\mathbf{y}$;

secondo passo: *scorrere la seconda colonna (delle sindromi) di M fino a trovare $S(\mathbf{y})$*;

terzo passo: *decodificare* $\mathbf{y}$ *come la differenza* $\mathbf{z}$ *tra* $\mathbf{y}$ *e la parola che si trova a sinistra di $S(\mathbf{y})$ nella matrice M.*

OSSERVAZIONE 281

Si noti che la parola $\mathbf{z}$ ottenuta alla fine di quest'algoritmo è la stessa che si otterrebbe usando il primo schema di decodifica con tabella standard.
Si noti ancora che, al fine della decodifica di $\mathbf{y}$, il primo algoritmo deve scorrere una tabella con q^{n-k} righe e q^k colonne, mentre il secondo soltanto la colonna delle sindromi, che ha q^{n-k} elementi. È chiaro quindi che, se C è abbastanza grande, il secondo algoritmo è più veloce del primo.

Consideriamo il $[4,2]-$codice binario

$$C = \{(0,0,0,0),(1,0,1,1),(0,1,0,1),(1,1,1,0)\}$$

avente come matrice controllo

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}.$$

Una tabella standard di C, ampliata mediante la colonna delle sindromi, è data da

$$\begin{array}{cccc|c} (0,0,0,0) & (1,0,1,1) & (0,1,0,1) & (1,1,1,0) & (0,0) \\ (1,0,0,0) & (0,0,1,1) & (1,1,0,1) & (0,1,1,0) & (1,1) \\ (0,1,0,0) & (1,1,1,1) & (0,0,0,1) & (1,0,1,0) & (0,1) \\ (0,0,1,0) & (1,0,0,1) & (0,1,1,1) & (1,1,0,0) & (1,0) \end{array}.$$

Consideriamo il $[5,2]-$codice binario

$$C = \{(0,0,0,0,0),(1,0,1,1,0),(0,1,0,1,1),(1,1,1,0,1)\},$$

per cui

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} \quad H = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Una tabella standard di C, ampliata mediante la colonna delle sindromi, è data da

00000	10110	01011	11101	**000**
10000	00110	11011	01101	**110**
01000	11110	00011	10101	**011**
00100	10010	01111	11001	**100**
00010	10100	01001	11111	**010**
00001	10111	01010	11100	**001**
10001	00111	10100	01100	**111**
11000	01110	10011	00101	**101**

3. I codici binari di Golay

indice

DEFINIZIONE 282

Il $[24, 12]$-codice esteso di $\mathcal{G}_{23}$ si chiama *codice binario di Golay esteso* e si denota con $\mathcal{G}_{24}$. Una sua matrice generatrice è data da

$$G_{24} = [I|A] = \left[\begin{array}{c|cccccccccccc} & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ I_{12} & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right].$$

PROPOSIZIONE 283

Il codice binario di Golay esteso $\mathcal{G}_{24}$ è autoduale e la matrice $[A|I]$ è una sua matrice generatrice.

DIMOSTRAZIONE

Ogni riga della matrice G_{24} è ortogonale a se stessa e a tutte le altre; ne segue che $\mathcal{G}_{24} \subseteq \mathcal{G}_{24}^{\perp}$. Allora, avendo $\mathcal{G}_{24}^{\perp}$ e $\mathcal{G}_{24}$ la stessa dimensione ($24 - 12 = 12$), risulta $\mathcal{G}_{24}^{\perp} = \mathcal{G}_{24}$.
D'altra parte, $[-A^t|I] = [A^t|I]$ è una matrice generatrice di $\mathcal{G}_{24}^{\perp} = \mathcal{G}_{24}$ e A è simmetrica ($A = A^t$). Ne segue la seconda parte dell'asserto.

Alcune proprietà delle parole binarie

DEFINIZIONE 284

Se $\mathbf{a}, \mathbf{b}$ sono parole binarie di lunghezza n, si denota con $\mathbf{a} \oplus \mathbf{b}$ la parola che nella $j-$esima posizione presenta 1 se, e solo se, $a_j = b_j = 1$, per ogni $j = 1, 2, \ldots, n$.

OSSERVAZIONE 285

Sia $X = \{x_1, x_2, \cdots, x_n\}$ un insieme linearmente ordinato con n elementi. Allora ogni parola binaria $\mathbf{a}$ di lunghezza n può essere riguardata come il vettore caratteristico del sottoinsieme $S(\mathbf{a}) = \{x_i \in X \ : \ a_i = 1\}$. Con questa identificazione, risulta

$$w(\mathbf{a}) = |S(\mathbf{a})| \quad e \quad S(\mathbf{a} \oplus \mathbf{b}) = S(\mathbf{a}) \cap S(\mathbf{b}),$$

ove $\mathbf{a}, \mathbf{b}$ sono parole binarie di lunghezza n.

ESEMPIO 286 $(1,1,0,1,0,1) \oplus (0,1,1,0,1,1) = (0,1,0,0,0,1)$.

Per $X = \{x_1, x_2, x_3, x_4, x_5, x_6\}$, $S(1,1,0,1,0,1) = \{x_1, x_2, x_4, x_6\}$.

PROPOSIZIONE 287

Se $\mathbf{a}, \mathbf{b}$ *sono parole binarie di lunghezza* n, *risulta*

1. $w(\mathbf{a}+\mathbf{b}) = w(\mathbf{a}) + w(\mathbf{b}) - 2w(\mathbf{a} \oplus \mathbf{b})$,
2. $\mathbf{ab} = \left(\sum_{j=1}^{n} a_j b_j\right) \ mod\, 2 = w(\mathbf{a} \oplus \mathbf{b}) \ mod\, 2$,
3. $\mathbf{ab} = 0 \ \Leftrightarrow \ w(\mathbf{a} \oplus \mathbf{b})$ *è pari*.

PROPOSIZIONE 288

Sia C un codice binario autoduale con matrice generatrice A avente tutte le righe di peso divisibile per 4. *Allora ogni parola di C ha peso divisibile per* 4 (codice doppiamente pari).

DIMOSTRAZIONE

Ricordiamo che ogni parola di C è somma di righe della matrice A e viceversa; inoltre, poiché C è autoduale, ogni sua parola ha peso pari. Se $\mathbf{a}$ e $\mathbf{b}$ sono righe di A è

$$w(\mathbf{a}+\mathbf{b}) = w(\mathbf{a}) + w(\mathbf{b}) - 2w(\mathbf{a}\oplus\mathbf{b})$$

e, essendo $\mathbf{ab} = 0$, $w(\mathbf{a}\oplus\mathbf{b})$ è pari e $w(\mathbf{a}+\mathbf{b})$ risulta divisibile per 4. Da questa osservazione segue che la somma di un qualunque insieme di righe di A ha peso divisibile per 4, cioè l'asserto.

PROPOSIZIONE 289

Il codice $\mathcal{G}_{24}$ ha distanza minima 8.

DIMOSTRAZIONE

$\mathcal{G}_{24}$ è autoduale e ogni riga di G_{24} ha peso divisibile per 4; ne segue che tutte le parole di $\mathcal{G}_{24}$ hanno peso divisibile per 4. Allora, dal momento che alcune righe di G_{24} hanno peso 8, basta provare che $\mathcal{G}_{24}$ non contiene parole di peso 4. A tale scopo rappresentiamo una parola $\mathbf{a} = a_1 a_2 \cdots a_{24} \in \mathcal{G}_{24}$ di peso 4 mediante due blocchi $\mathbf{a} = (\mathbf{s}, \mathbf{d})$, ove $\mathbf{s} = a_1 \cdots a_{12}$ e $\mathbf{d} = a_{13} \cdots a_{24}$ ed esaminiamo i possibili casi.

DIMOSTRAZIONE (CONTINUAZIONE) 290

- $w(\mathbf{s}) = 0, w(\mathbf{d}) = 4$*: Impossibile perchè* $\mathbf{0}$ *è l'unica parola con* $w(\mathbf{s}) = 0$ *: per provarlo basta riferirsi alla matrice generatrice* G_{24}.
- $w(\mathbf{s}) = 1, w(\mathbf{d}) = 3$*: Se* $w(\mathbf{s}) = 1$, $\mathbf{a}$ *è una riga di* G_{24} *e nessuna di queste ha peso* 4.
- $w(\mathbf{s}) = 2, w(\mathbf{d}) = 2$*: Se* $w(\mathbf{s}) = 2$, $\mathbf{a}$ *è somma di due righe di* G_{24} *e nessuna di tali somme ha peso* 4.
- $w(\mathbf{s}) = 3, w(\mathbf{d}) = 1$*: Se* $w(\mathbf{d}) = 1$, $\mathbf{a}$ *è una riga della matrice generatrice* $[A|I]$ *e nessuna di queste ha peso* 4.
- $w(\mathbf{s}) = 4, w(\mathbf{d}) = 0$*: Impossibile perché* $\mathbf{0}$ *è l'unica parola con* $w(\mathbf{d}) = 0$ *: per provarlo basta riferirsi alla matrice generatrice* $[A|I]$.

PROPOSIZIONE 291

Il codice binario di Golay $\mathcal{G}_{23}$ ha distanza minima 7 ed è perfetto (come avevamo preannunziato).

DIMOSTRAZIONE

Abbiamo provato che $\mathcal{G}_{24}$, codice esteso di $\mathcal{G}_{23}$, ha distanza minima 8; da qui segue subito che il codice binario di Golay ha distanza minima 7 e, quindi, è un $[23, 12, 7]$-codice binario $3-$correttore. La disuguaglianza di Hamming, in questo caso diventa un'uguaglianza:

$$2^{12}\left[\binom{23}{0}+\binom{23}{1}+\binom{23}{2}+\binom{23}{3}\right]=$$

$$2^{12}\left[1+23+11\cdot 23+7\cdot 11\cdot 23\right]=2^{12}2048=2^{12}2^{11}=2^{23}.$$

OSSERVAZIONE 292

A volte, come nel caso del codice binario di Golay, conviene ricercare le proprietà di un codice attraverso lo studio del codice esteso.

4. Relazione fondamentale tra distanza minima e matrici di controllo

indice

CONVENZIONE 293

Nella proposizione 294 che segue:

- C denota un $[n, n-m]-$codice su F_q,
- $H = (a_{ij})$ una matrice controllo di parità di C,
- $\mathbf{a}^1, \mathbf{a}^2, ..., \mathbf{a}^n$ i vettori di lunghezza m corrispondenti alle colonne della matrice H.

PROPOSIZIONE 294

Valgono le seguenti proprietà:
(1) *Se* $\mathbf{x}$ *è una parola di* C *di peso* $t > 0$ *e se* $x_{i_1}, x_{i_2}, .., x_{i_t}$ *sono le sue componenti diverse da zero, allora le colonne* $\mathbf{a}^{i_1}, \mathbf{a}^{i_2}, \ldots, \mathbf{a}^{i_t}$ *di* H *sono linearmente dipendenti di* F_q^m.
(2) *Se* $x_{i_1}, x_{i_2}, \ldots, x_{i_t}$ *sono elementi di* F_q *non tutti nulli tali che*

$$\sum_{j=1}^{t} x_{i_j} \mathbf{a}^{i_j} = \mathbf{0},$$

allora la parola $\mathbf{x} \in F_q^n$ *di componenti*

$$x_s = \begin{cases} 0 & \text{se } s \neq i_1, i_2, \ldots, i_t, \\ x_{i_j} & \text{se } s = i_j \text{ , con } j = i_1, i_2 \ldots, i_t. \end{cases}$$

è una parola del codice C *di peso al più* t.

Nell'ipotesi (1), abbiamo:

$$x_{i_1}\mathbf{a}^{i_1} + x_{i_2}\mathbf{a}^{i_2} + \cdots + x_{i_t}\mathbf{a}^{i_t} =$$

$$(x_{i_1}a_{1i_1} + x_{i_2}a_{1i_2} + \cdots + x_{i_t}a_{1i_t}, \ldots, x_{i_1}a_{mi_1} + x_{i_2}a_{mi_2} + \cdots + x_{i_t}a_{mi_t}) =$$

$$\left(\sum_{j=1}^{t} x_{i_j}a_{1i_j}, \sum_{j=1}^{t} x_{i_j}a_{2i_j}, \ldots, \sum_{j=1}^{t} x_{i_j}a_{mi_j}\right) = \left(\sum_{j=1}^{n} x_j a_{1j}, \sum_{j=1}^{n} x_j a_{2j}, \ldots, \sum_{j=1}^{n} x_j a_{mj}\right) =$$

$$(x_1, x_2, \ldots, x_n)\begin{bmatrix} a_{11} & a_{21} & \ldots & a_{m1} \\ a_{12} & a_{22} & \ldots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \ldots & a_{mn} \end{bmatrix} = \mathbf{x}H^t = \mathbf{0} \text{ (perché } \mathbf{x} \in C).$$

Le colonne $\mathbf{a}^{i_1}, \mathbf{a}^{i_2}, .., \mathbf{a}^{i_t}$ di H sono, dunque, linearmente dipendenti.

Nell'ipotesi (2), abbiamo:

$$\mathbf{x}H^t = (x_1, x_2, \ldots, x_n) \begin{bmatrix} a_{11} & a_{21} & \ldots & a_{m1} \\ a_{12} & a_{22} & \ldots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \ldots & a_{mn} \end{bmatrix} =$$

$$\left(\sum_{j=1}^{n} x_j a_{1j}, \sum_{j=1}^{n} x_j a_{2j}, \ldots, \sum_{j=1}^{n} x_j a_{mj} \right) = \left(\sum_{j=1}^{t} x_{i_j} a_{1 i_j}, \sum_{j=1}^{t} x_{i_j} a_{2 i_j}, \ldots, \sum_{j=1}^{t} x_{i_j} a_{m i_j} \right) =$$

$$\left(x_{i_1} a_{1 i_1} + x_{i_2} a_{1 i_2} + \cdots + x_{i_t} a_{1 i_t}, \ldots, x_{i_1} a_{m i_1} + x_{i_2} a_{m i_2} + \cdots + x_{i_t} a_{m i_t} \right) =$$

$$x_{i_1} \mathbf{a}^{i_1} + x_{i_2} \mathbf{a}^{i_2} + \cdots + x_{i_t} \mathbf{a}^{i_t} = \mathbf{0} \;\Rightarrow\; \mathbf{x} \in C.$$

OSSERVAZIONE 295

Nelle ipotesi (2), il peso della parola $\mathbf{x}$ è pari al numero degli scalari $x_{i_1}, x_{i_2}, \ldots, x_{i_t}$ diversi da zero.

Distanza minima e matrici di controllo

I due teoremi che seguono sono immediati corollari della proposizione 294.

PROPOSIZIONE 296

Siano C un $[n, n-m]-$codice su F_q, H una sua matrice di controllo e t un intero positivo. Allora

1. *la distanza minima di C è $\geq t$ se, e soltanto se, ogni insieme di $t-1$ colonne di H è linearmente indipendente;*
2. *la distanza minima di C è $\leq t$ se, e soltanto se, esistono t colonne di H linearmente dipendenti.*

PROPOSIZIONE 297

Siano C un $[n, n-m]-$codice su F_q e H una sua matrice di controllo. Allora C ha distanza minima d se, e soltanto se, le colonne di H generano F_q^m e d è il minimo numero di colonne dipendenti di H, cioè:

1. *$d-1$ colonne arbitrarie di H sono indipendenti,*
2. *esistono in H d colonne dipendenti.*

ESEMPIO 298

Le colonne della matrice

$$H = \begin{bmatrix} -1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & -1 \\ 0 & -1 & 1 & 0 & 0 \end{bmatrix}$$

sono a due a due indipendenti sul campo $F_3 = \{0, 1, -1\}$ e ne esistono tre dipendenti (le prime tre!).
Ne segue che il $[5, 2]-$codice lineare avente H come matrice di controllo ha distanza minima 3.

Il codice ternario di Golay

Le colonne della matrice

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & -1 & -1 \\ 0 & 0 & 1 & 0 & 0 & 1 & -1 & -1 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & -1 & 1 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & -1 & -1 & 1 & 0 \end{bmatrix}$$

sono a quattro a quattro indipendenti sul campo $F_3 = \{0, 1, -1\}$ e ne esistono cinque dipendenti (prima, seconda, quarta, quinta, nona!). Il codice lineare avente H come matrice di controllo ha parametri $[11, 6, 5]$ ed è perfetto:

$$3^6 \left[\binom{11}{0} + \binom{11}{1} 2 + \binom{11}{2} 2^2 \right] = 3^6 \left[1 + 22 + 220 \right] = 3^6 3^5 = 3^{11}.$$

Tale codice è noto come *codice ternario di Golay* e si denota con $\mathcal{G}_{11}$.

5. Il problema fondamentale della teoria dei codici lineari

indice

Abbiamo visto che le colonne di una matrice di controllo di un $[n, n-m, d]-$codice su F_q costituiscono un insieme Γ di n vettori di F_q^m con le seguenti proprietà:

$$\begin{cases} \Gamma \text{ è un generatore di } F_q^m, \\ \text{ogni } d-1 \text{ vettori di } \Gamma \text{ sono indipendenti,} \\ \text{in } \Gamma \text{ esistono } d \text{ vettori dipendenti.} \end{cases} \quad (38)$$

DEFINIZIONE 299

Un insieme Γ di n vettori di F_q^m si dice $(n, d-1)-$*insieme* se sono verificate le seguenti proprietà:

$$\begin{cases} \Gamma \text{ è un generatore di } F_q^m, \\ \text{ogni } d-1 \text{ vettori di } \Gamma \text{ sono indipendenti,} \\ \text{in } \Gamma \text{ esistono } d \text{ vettori dipendenti.} \end{cases} \quad (39)$$

PROPOSIZIONE 300

Esiste un $[n, n-m, d]-$codice su F_q se, e solo se, esiste in F_q^m un $(n, d-1)$-insieme.

DIMOSTRAZIONE

Siano Γ un $(n, d-1)$-insieme di F_q^m e H la matrice avente per colonne i vettori di Γ. Allora le colonne di H generano F_q^m e sono a $d-1$ a $d-1$ indipendenti. Esistono, inoltre, d colonne di H dipendenti. Allora il codice avente H come controllo di parità ha parametri $[n, n-m, d]$. Viceversa, sappiamo che le colonne di una matrice di controllo di un $[n, n-m, d]-$codice su F_q sono un $(n, d-1)$-insieme di F_q^m.

DEFINIZIONE 301

Il massimo valore di n per cui esiste in F_q^m un $(n, d-1)$-insieme si denota con

$$max_{d-1}(m, q)$$

Un $(n, d-1)$-insieme con $n = max_{d-1}(m, q)$ si dice *ottimo*.

PROBLEMA 302

[R.C.Bose, 1947] Fissati m e q, il problema di determinare $max_{d-1}(m,q)$ e tutti gli $(n, d-1)$-insiemi ottimi di F_q^m è noto come *packing problem* **(PP)**.

PROBLEMA 303

Fissati m, d, q, con $d \leq m+1$, il problema di calcolare il più grande intero n per cui esiste un codice su F_q con parametri $[n, n-m, d]$ è noto come *problema fondamentale della teoria dei codici lineari* **(PFTCL)**.

Quanto finora mostrato può sintetizzarsi nel risultato seguente.

TEOREMA 304

Fissati m, d, q, con $d \leq m+1$, il massimo intero n per cui esiste un codice su F_q con parametri $[n, n-m, d]$ è uguale al numero di vettori di un $(n, d-1)$-insieme ottimo in F_q^m; cioè a $max_{d-1}(m,q)$. In altre parole, PP è equivalente a PFTCL .

Packing problem

Il packing problem, cioè il calcolo di $max_{d-1}(m, q)$ (massimo valore di n per cui esiste in F_q^m un $(n, d-1)$-insieme), è un problema molto difficile.

Valori noti di $max_{d-1}(m, q)$

m	q	$d-1$	$max_{d-1}(m, q)$	
		2	$\frac{q^m-1}{q-1}$	
	2	3	2^{m-1}	*Bose* 1947
3	*pari*	3	$q+2$	*Bose* 1947
3	*dispari*	3	$q+1$	*Bose* 1947
4	*dispari*	3	q^2+1	*Bose* 1947
4	*pari* > 2	3	q^2+1	*Qvist* 1952
5	3	3	20	*Pellegrino* 1970
6	3	3	56	*Hill* 1973

6. CODICI MDS

indice

OSSERVAZIONE 305

Ricordiamo che un codice lineare C su F_q di parametri $[n, n-m, d]$ è $(n-m)-$sistematico. Per un tale codice, quindi, la disuguaglianza di Singleton si scrive

$$d \leq n-(n-m)+1 = m+1. \tag{40}$$

La (40) segue anche dal fatto che le colonne di una matrice di controllo di C sono vettori di F_q^m a $d-1$ a $d-1$ indipendenti ed m è il massimo numero di vettori indipendenti di F_q^m.

OSSERVAZIONE 306

I codici per i quali la (40) è un'uguaglianza, cioè i codici con parametri $[n, n-m, m+1]$ li abbiamo definiti *codici ottimali,* o *MDS,* o *MDS-codici* (*MDS* sta per *maximum distance separable*).
Poiché la capacità di correggere errori è funzione crescente della distanza minima, tra i codici di lunghezza n e dimensione $n-m$ fissate, quelli MDS sono quelli che hanno la massima capacità di correggere errori.

OSSERVAZIONE 307

Un $[n, k, d]-$codice è *MDS* se, e solo se, $d = n - k + 1$.

ESEMPI (Codici *MDS* banali) 308

1. $V(n, q)$ è un $[n, n] -$ *codice MDS* perché ha peso minimo 1.
2. Il codice di ripetizione $C(q, n)$ di lunghezza n su F_q è un $[n, 1]-$codice *MDS* perché ha peso minimo n.
3. Il codice costituito dalle parole di lunghezza n la cui somma delle componenti è zero è $C(q, n)^{\perp}$ (codice ortogonale a quello di ripetizione $C(q, n)$ di lunghezza n su F_q). In esso una parola di peso minimo ha due componenti non nulle, una l'opposta dell'altra, e tutte le altre uguali a zero. Allora $C(q, n)^{\perp}$ è *MDS*, avendo parametri $[n, n-1, 2]$ ed è *MDS*.

PROPOSIZIONE 309

Siano $a_1, a_2, \ldots, a_m$ elementi distinti e non nulli di un campo. Allora la matrice (di **Vandermonde***)*

$$A = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_m \\ a_1^2 & a_2^2 & \ldots & a_m^2 \\ \vdots & \vdots & \ldots & \vdots \\ \vdots & \vdots & \ldots & \vdots \\ a_1^{m-1} & a_2^{m-1} & \ldots & a_m^{m-1} \end{bmatrix},$$

ha determinante non nullo e risulta

$$\det A = \prod_{i<j} (a_j - a_i).$$

DIMOSTRAZIONE

Sottraendo ad ogni riga di A, diversa dalla prima, a_1 per la riga precedente, si ha

$$\det A = \det \begin{bmatrix} 1 & 1 & \dots & 1 \\ 0 & a_2 - a_1 & \dots & a_m - a_1 \\ 0 & a_2(a_2 - a_1) & \dots & a_m(a_m - a_1) \\ \vdots & \vdots & \dots & \vdots \\ \vdots & \vdots & \dots & \vdots \\ 0 & a_2^{m-2}(a_2 - a_1) & \dots & a_m^{m-2}(a_m - a_1) \end{bmatrix}$$

DIMOSTRAZIONE (CONTINUAZIONE)

$$= \det \begin{bmatrix} 1 & 1 & \dots & 1 \\ a_2 & a_3 & \dots & a_m \\ a_2^2 & a_3^2 & \dots & a_m^2 \\ \vdots & \vdots & \dots & \vdots \\ \vdots & \vdots & \dots & \vdots \\ a_2^{m-2} & a_3^{m-2} & \dots & a_m^{m-2} \end{bmatrix} \prod_{j=2}^{m} (a_j - a_1).$$

A questo punto l'asserto si ottiene facilmente per induzione su m.

ESEMPIO 310

Consideriamo la seguente matrice di Vandermonde sul campo $Z_5 = \{0, 1, 2, 3, 4\}$

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1^2 & 2^2 & 3^2 & 4^2 \\ 1^3 & 2^3 & 3^3 & 4^3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 4 & 4 & 1 \\ 1 & 3 & 2 & 4 \end{bmatrix}.$$

Risulta:

$$\det A = (4-3)(4-2)(4-1)(3-2)(3-1)(2-1) =$$

$$1 \cdot 2 \cdot 3 \cdot 1 \cdot 2 \cdot 1 = 2.$$

PROPOSIZIONE 311

Siano $a_1, a_2, \ldots, a_{m-1}$ elementi distinti e non nulli di un campo. Allora le matrci

$$\begin{bmatrix} 1 & 1 & \ldots & 1 & 1 \\ a_1 & a_2 & \ldots & a_{m-1} & 0 \\ a_1^2 & a_2^2 & \ldots & a_{m-1}^2 & 0 \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ a_1^{m-1} & a_2^{m-1} & \ldots & a_{m-1}^{m-1} & 0 \end{bmatrix} \quad e \quad \begin{bmatrix} 1 & 1 & \ldots & 1 & 0 \\ a_1 & a_2 & \ldots & a_{m-1} & 0 \\ a_1^2 & a_2^2 & \ldots & a_{m-1}^2 & 0 \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ a_1^{m-1} & a_2^{m-1} & \ldots & a_{m-1}^{m-1} & 1 \end{bmatrix}$$

hanno determinante non nullo.

DIMOSTRAZIONE

Segue facilmente dalla proposizione sul determinante di Vandermonde.

Esempio di codice MDS

Siano $a_1, a_2, \ldots, a_{q-1}$ gli elementi non nulli del campo F_q e in F_q^m, con $2 \leq m \leq q$, consideriamo l'insieme di $q+1$ vettori

$$X = \{(1, t, t^2, ..., t^{m-1}) \ : \ t \in F_q\} \cup \{(0, \ldots, 0, 1)\} \text{ (\textit{curva razionale normale}).}$$

La matrice avente per colonne i vettori di X

$$H = \begin{bmatrix} 1 & 1 & \ldots & 1 & 1 & 0 \\ a_1 & a_2 & \ldots & a_{q-1} & 0 & 0 \\ a_1^2 & a_2^2 & \ldots & a_{q-1}^2 & 0 & 0 \\ \vdots & \vdots & \ldots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \ldots & \vdots & \vdots & \vdots \\ a_1^{m-1} & a_2^{m-1} & \ldots & a_{q-1}^{m-1} & 0 & 1 \end{bmatrix},$$

ha le colonne a m a m indipendenti ed ha rango m. Allora il codice lineare su F_q avente H come matrice di controllo ha parametri $[q+1, q+1-m, m+1]$ ed è un codice MDS.

Esempio di codice MDS

Siano $a_1, a_2, \ldots, a_{q-1}$ gli elementi non nulli del campo F_q e in F_q^3, con q pari, consideriamo l'insieme di $q+2$ vettori (*iperovale regolare*)

$$X = \left\{(1, t, t^2) \ : \ t \in F_q\right\} \cup \{(0,0,1),(0,1,0)\}\,.$$

Se $a_1, a_2, \ldots, a_{q-1}$ sono gli elementi non nulli del campo F_q, sappiamo che le prime $q+1$ colonne della matrice

$$H = \begin{bmatrix} 1 & 1 & \ldots & 1 & 1 & 0 & 0 \\ a_1 & a_2 & \ldots & a_{q-1} & 0 & 0 & 1 \\ a_1^2 & a_2^2 & \ldots & a_{q-1}^2 & 0 & 1 & 0 \end{bmatrix},$$

sono a 3 a 3 indipendenti. Inoltre, con $i \neq j$, risulta

$$\det \begin{bmatrix} 1 & 1 & 0 \\ a_i & a_j & 1 \\ a_i^2 & a_j^2 & 0 \end{bmatrix} = a_i^2 + a_j^2 = (a_i + a_j)^2 \neq 0.$$

Ne segue che in F_q^3 l'insieme di $q+2$ vettori di X è un $(q+2,3)-$insieme. Allora il codice lineare su F_q avente H come matrice di controllo ha parametri $[q+2, q-1, 4]$ ed è un codice MDS.

7. $max_2(m, q)$ e i codici di Hamming

indice

OSSERVAZIONE 312

$max_2(m,q)$ è il massimo numero di vettori non nulli di F_q^m a due a due indipendenti (non proporzionali), cioè non appartenenti ad uno stesso sottospazio vettoriale $1-$dimensionale. Ne segue che:

- un $(n,2)-$insieme ottimo si ottiene prendendo un vettore non nullo in ciascuno dei sottospazi $1-$dimensionali di $V(n,q)$.
- $max_2(m,q)$ è uguale al numero dei sottospazi $1-$dimensionali di F_q^m;

PROPOSIZIONE 313

Il numero di sottospazi $1-$*dimensionali di* F_q^m *è*

$$\frac{q^m-1}{q-1} = q^{m-1} + q^{m-2} + \cdots + q + 1. \tag{41}$$

DIMOSTRAZIONE

Ogni sottospazio di dimensione 1 contiene $q-1$ vettori non nulli e tali sottospazi, privati del vettore nullo, formano una partizione dei q^m-1 vettori non nulli di F_q^m.

PROPOSIZIONE 314

Un $(n, 2)-$insieme ottimo si ottiene prendendo un vettore non nullo in ciascuno dei sottospazi $1-$dimensionali di F_q^n. Di conseguenza, l'intero $max_2(m, q)$ è uguale al numero dei sottospazi $1-$dimensionali di F_q^m; cioè:

$$max_2(m, q) = \frac{q^m - 1}{q - 1}. \tag{42}$$

CONCLUSIONE 315

Fissati m e q, la (42) fornisce il massimo intero n per cui esiste un $[n, n-m, 3]-$codice su F_q. Un tale codice, che risulta $1-$correttore, si chiama $(m, q)-$*codice di Hamming* e si denota con $Ham(m, q)$.

Costruzione di $Ham(m, q)$

Posto $n = q^{m-1} + q^{m-2} + \cdots + q + 1$, siano $V_1(1, q), V_2(1, q), \ldots, V_n(1, q)$ i sottospazi di F_q^m di dimensione 1.
Per $i = 1, 2, \cdots n$, sia $\mathbf{a}^i = (a_{1i}, a_{2i}, ..., a_{mi}) \in V_i(1, q) \setminus \{\mathbf{0}\}$. Denotata con $H = H_{m,q} = (a_{ij})$ la matrice di tipo $m \times n$ avente come vettori colonna $\mathbf{a}^1, \mathbf{a}^2, ..., \mathbf{a}^n$, $Ham(m, q)$ è il codice lineare avente H come matrice controllo di parità, cioè

$$Ham(m, q) = \{\mathbf{a} \in F_q^n \ : \ \mathbf{a}H^t = \mathbf{0}\}.$$

PROPOSIZIONE 316

Il codice $Ham(m, q)$ è perfetto.

DIMOSTRAZIONE

Poiché $Ham(m, q)$ è $1-$correttore, le sfere di centro le sue parole e raggio 1 sono a due a due disgiunte e ognuna di esse contiene esattamente $n(q - 1) + 1$ parole di F_q^n. Ne segue che:

$$q^{n-m}[1 + n(q - 1)] = q^n = |F_q^n|.$$

Risultati sui codici perfetti (non necessariamente lineari)

J.H.van Lint, A.Tietäväinen (1973-75)

TEOREMA 317

Ogni codice $q-$ario perfetto non banale, con q potenza di un primo, ha i parametri di un codice di Hamming o di Golay.

J.L.Vasil'ev (1962), J.Schönheim (1968)
B.Lindstrom (1969)

TEOREMA 318

Esistono codici perfetti non banali con gli stessi parametri dei codici di Hamming.

V.Pless (1968), S.L.Snover (1973)
P.Delsarte e J.M.Goethals (1975)

TEOREMA 319

Ogni codice con i parametri di un codice di Golay è equivalente al codice di Golay con gli stessi parametri.

M.R.Best (1983), Y.Hong (1984)$[e = 6, 8]$

TEOREMA 320

Se C è un codice $q-$ario perfetto non banale ed $e-$correttore, con $e \geq 3$, allora è $q = 2$ e C è equivalente al codice binaro di Golay $\mathcal{G}_{23}$.

CONGETTURA 321

Per $e = 1, 2$, non esistono codici perfetti non banali ed $e-$correttori su alfabeti il cui ordine non sia la potenza di un primo.

OSSERVAZIONE 322

Codici di Hamming su F_q con gli stessi parametri sono equivalenti.

TEOREMA 323

I codici lineari perfetti non banali sono tutti e soli i codici di Hamming e i codici di Golay $\mathcal{G}_{23}$ e $\mathcal{G}_{11}$.

OSSERVAZIONE 324

I codici di Golay $\mathcal{G}_{24}$ (estensione di $\mathcal{G}_{23}$) e $\mathcal{G}_{11}$ furono descritti per la prima volta da M.Golay in un articolo di sole due pagine [1] ("*Notes on Digital Coding*", Proc. IRE 37: 657). Il codice $\mathcal{G}_{24}$ può essere costruito anche geometricamente utilizzando un poliedro detto "grande dodecaedro" [2].

[1] http://www.maths.manchester.ac.uk/~ybazlov/code/golay_paper.pdf

[2] http://blogs.ams.org/visualinsight/2015/12/01/golay-code

La matrice

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} = [-A^t, I_2]$$

è un controllo di parità di $Ham(2,2)$, che è il più piccolo codice di Hamming. Dalla forma di H si ha che una matrice generatrice di $Ham(2,2)$ è

$$G = [I_1, A] = [1 \;\; 1 \;\; 1] .$$

Ne segue che $Ham(2,2)$ è il codice di ripetizione binario di lunghezza 3 :

$$Ham(2,2) = \{(0,0,0) , (1,1,1)\} .$$

Il codice di Hamming $Ham(3,2)$

La matrice

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} = [-A^t, I_3]$$

è un controllo di parità del codice $Ham(3,2)$. Dalla forma di H si ha che una matrice generatrice di $Ham(3,2)$ è

$$G = [I_4, A] = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

OSSERVAZIONE 325

Il codice di Hamming $Ham(3,2)$ è il più piccolo codice perfetto non banale.

ESEMPIO 326

I due esempi precedenti si generalizzano nel seuente modo. Sia A_m una matrice che ha per righe tutte le parole binarie di lunghezza m e peso maggiore di 1. Allora, la matrice

$$H = H_{m,2} = [-A_m^t, I_m]$$

è un controllo di parità del codice $Ham(m, 2)$. Dalla forma di H si ha che una matrice generatrice di $Ham(m, 2)$ è

$$G = [I_{n-m}, A_m],$$

con $n = 2^m - 1$.

OSSERVAZIONE 327

Una parola **a** di $Ham(m, q)$ ha peso $c > 0$ e presenta lettere diverse da zero nelle posizioni $i_1, i_2, ..., i_c$ se, e soltanto se, le colonne di posto $i_1, i_2, ..., i_c$ in H sono linearmente dipendenti (Prop.294).

OSSERVAZIONE 328

La matrice $H_{m,2}$ ha per colonne tutti i vettori non nulli di Z_2^m. Se interpretiamo ciascuna di queste colonne come la rappresentazione binaria di un intero (compreso fra 1 ed $n = 2^m - 1$), possiamo ordinare le colonne di $H_{m,2}$ secondo l'ordine crescente degli interi che rappresentano.

ESEMPIO 329

Per $m = 2$ si ha:

$$(1)_2 = 01\,,\ (2)_2 = 10\,,\ (3)_2 = 11\,;$$

$$H_{2,2} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

ESEMPIO 330

Per $m = 3$ si ha:

$$(1)_2 = 001\,,\ (2)_2 = 010\,,\ (3)_2 = 011\,,\ (4)_2 = 100\,,$$

$$(5)_2 = 101\,,\ (6)_2 = 110\,,\ (7)_2 = 111\,;$$

$$H_{3,2} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Decodifica con $Ham(m, 2)$

OSSERVAZIONE 331

- $Ham(m, 2)$ è un $[n, n-m, 3]-$codice, con $n = 2^m - 1$.
- Il numero di laterali di $Ham(m, 2)$ in Z_2^n è $\frac{2^n}{2^{n-m}} = 2^m = n + 1$ e ciascun laterale proprio contiene un'unica parola delle n di peso 1 (altrimenti $Ham(m, 2)$, che ha peso minimo 3, conterrebbe una parola di peso 2.).
- Le direttrici dei laterali propri in una tabella standard di $Ham(m, 2)$ sono tutte e sole le $2^m - 1$ parole $\mathbf{j} = (0, .., 0, 1, 0, .., 0)$ (con 1 nella $j-$ma posizione).
- La sindrome di $\mathbf{j}$, e quindi di ogni parola appartenente al laterale $\mathbf{j} + Ham(m, q)$, è esattamente il vettore trasposto della $j-$ma colonna di H.
- Scriviamo H in ordine crescente delle sue colonne, considerate come rappresentazioni binarie di interi e sia $\mathbf{x} \in Ham(m, 2)$. Se $d(\mathbf{x}, \mathbf{y}) = 1$ e $S(\mathbf{y}) = S(\mathbf{j})$, allora $\mathbf{y} + \mathbf{j} \in Ham(m, 2)$ e, quindi, $\mathbf{x}$ differisce da $\mathbf{y}$ sulla $j-$esima posizione. In altri termini: se su una parola $\mathbf{x} \in Ham(m, 2)$ si cambia la componente $j-$esima ottenendo la parola $\mathbf{y}$, risulta $S(\mathbf{y}) = S(\mathbf{j})$, e viceversa.

Decodifica con $Ham(m, 2)$

In un canale di trasmissione binario, che commette non più di un errore sulle parole di lunghezza $n = 2^m - 1$ e che lavora con il codice $Ham(m, 2)$, si può usare il seguente algoritmo di decodifica, ove $\mathbf{y}$ è la parola ricevuta e $\mathbf{z}$ la decodifica di $\mathbf{y}$:

primo passo: Calcolare la sindrome $S(\mathbf{y})$.

secondo passo: Se $S(\mathbf{y}) = \mathbf{0}$, si ponga $\mathbf{z} = \mathbf{y}$.

terzo passo: Se $S(\mathbf{y}) \neq \mathbf{0}$, si calcoli il numero intero j rappresentato in binario da $S(\mathbf{y})$ e si ponga $\mathbf{z} = \mathbf{j} + \mathbf{y}$ (cambiare la lettera di posto j in $\mathbf{y}$).

OSSERVAZIONE 332

Quello appena descritto è una variante dell'algoritmo di decodifica a sindromi ma, a differenza di quest'ultimo, è veloce perché, per trovare la riga della tabella standard di C cui $\mathbf{y}$ appartiene (cioè $\mathbf{j}$) non è necessario scorrere la colonna delle sindromi: basta solo trovare la sindrome di $\mathbf{y}$ (un prodotto di matrici).

Nel caso $m = 3$, per la decodifica veloce con $Ham(3, 2)$, bisogna considerare la matrice di controllo

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Se $\mathbf{y} = 1101011$ è la parola ricevuta, si calcola $S(\mathbf{y}) = 110$, che risulta la rappresentazione binaria di 6. Se ne deduce, allora, che è stato commesso un errore nella sesta posizione. La parola $\mathbf{y}$ viene così decodificata con $\mathbf{z} = 1101001$:
$\mathbf{y} = 1101011 \to (1, 1, 0, 1, 0, 1, 1)H^t = (1, 1, 0) \to 110 = (6)_2 \to$
$\mathbf{z} = 1101001$

8. $max_3(m, q)$

indice

OSSERVAZIONE 333

Un sottospazio $k-$dimensionale di F_q^m ha ordine q^k. In particolare, i sottospazi di dimensione 1 e 2 contengono rispettivamente q e q^2 vettori.

PROPOSIZIONE 334

Il numero di sottospazi $2-$*dimensionali di* F_q^m *contenenti un fissato sottospazio* $1-$*dimensionale è*

$$\frac{q^{m-1}-1}{q-1} = q^{m-2} + q^{m-3} + \cdots + q + 1. \tag{43}$$

DIMOSTRAZIONE

I sottospazi $2-$dimensionali di F_q^m contenenti un fissato sottospazio $1-$dimensionale V_1, sono un ricoprimento di F_q^m e a due a due s'intersecano in V_1. Il numero ν di tali sottospazi verifica, pertanto, l'uguaglianza

$$\mid F_q^m \setminus V_1 \mid = q^m - q = \nu(q^2 - q)$$

e, da questa, si ha subito l'asserto.

PROPOSIZIONE 335

Un insieme di vettori Γ *di* F_q^m *è un* $(n, 3)-$*insieme se, e sole se, ogni sottospazio vettoriale* $2-$*dimensionale interseca* Γ *in* $0, 1$ *o* 2 *vettori. Risulta, inoltre,*

$$max_3(m, q) \leq \frac{q^{m-1} - 1}{q - 1} + 1. \tag{44}$$

DIMOSTRAZIONE

Un $(n, 3)-$insieme Γ di F_q^m è un insieme di vettori a tre a tre indipendenti (quindi non nulli), cioè non appartenenti ad uno stesso sottospazio vettoriale $2-$dimensionale; ne segue la prima parte dell'asserto.
Ora, detto $V_1 =< \mathbf{a} >$ un sottospazio $1-$dimensionale contenente un fissato vettore $\mathbf{a}$ di Γ, ogni sottospazio 2 dimensionale contenente V_1 contiene al più un altro vettore di Γ diverso da $\mathbf{a}$. Dalla (43), allora, abbiamo

$$\mid \Gamma \mid \leq \frac{q^{m-1} - 1}{q - 1} + 1$$

e, ricordando che $max_3(m, q)$ è il numero di vettori di un $(m, q)-$insieme ottimale, si ha subito la (44).

OSSERVAZIONE 336

Nel caso $q = 2$, la (44), diventa $max_3(m, 2) \leq 2^{m-1}$.

PROPOSIZIONE 337

L'insieme Γ *dei vettori di* Z_2^m *non appartenenti ad un fissato sottospazio* V_{m-1} *di dimensione* $m - 1$ *è un* $(2^{m-1}, 2)$*-insieme.*

DIMOSTRAZIONE

Osserviamo che ogni sottospazio $2-$dimensionale contiene esattamente 4 vettori, di cui 3 non nulli. Detto V_2 un tale sottospazio non contenuto in V_{m-1}, risulta

$$dim(V_2 \cap V_{m-1}) = 1$$

e, quindi, ogni V_2 ha soltanto 2 vettori in comune con $\Gamma = V(m, 2) \setminus V_{m-1}$. Ne segue l'asserto.

TEOREMA 338

$$max_3(m, 2) = 2^{m-1}. \tag{45}$$

OSSERVAZIONE 339

Nel caso $m = 3$ la disuguaglianza

$$max_3(m, q) \leq \frac{q^{m-1} - 1}{q - 1} + 1$$

diventa

$$max_3(3, q) \ \leq \ q + 2. \tag{46}$$

TEOREMA 340

Se q è pari, risulta:

$$max_3(3, q) \ = \ q + 2. \tag{47}$$

Se q è dispari, risulta:

$$max_3(3, q) \ = \ q + 1. \tag{48}$$

Se $a_1, a_2, \ldots, a_{q-1}$ sono gli elementi non nulli del campo F_q, sappiamo che la matrice

$$H = \begin{bmatrix} 1 & 1 & \ldots & 1 & 1 & 0 \\ a_1 & a_2 & \ldots & a_{q-1} & 0 & 0 \\ a_1^2 & a_2^2 & \ldots & a_{q-1}^2 & 0 & 1 \end{bmatrix},$$

ha le colonne a 3 a 3 indipendenti ed ha rango 3. Inoltre, con $i \neq j$, risulta

$$\det \begin{bmatrix} 1 & 1 & 0 \\ a_i & a_j & 1 \\ a_i^2 & a_j^2 & 0 \end{bmatrix} = a_i^2 + a_j^2 = (a_i + a_j)^2 \neq 0.$$

Ne segue che in F_q^3 l'insieme di $q + 2$ vettori

$$X = \{(1, t, t^2) \ : \ t \in F_q\} \cup \{(0, 0, 1), (0, 1, 0)\}$$

è un $(q + 2, 3)-$insieme. Dalla (46) segue, allora, l'asserto.

Sappiamo che in F_q^3 l'insieme dei $q + 1$ vettori

$$X = \{(1, t, t^2) \ : \ t \in F_q\} \cup \{(0, 0, 1)\}$$

è un $(q + 1, 3)-$insieme.
Supponiamo, ora, che esista un $(q + 2, 3)-$insieme Γ e osserviamo che ogni sottospazio di dimensione 2 interseca Γ in 0 o 2 vettori. Allora, detto t il numero dei sottospazi $2-$dimensionali incidenti Γ e contenenti un fissato vettore $\mathbf{a} \notin \Gamma$, deve essere

$$2t = q + 2$$

e ciò è assurdo, essendo $q + 2$ dispari. Ne segue che, nelle nostre ipotesi, non possono esistere $(q + 2, 3)-$insiemi e, così abbiamo l'asserto.

9. Il gioco dei cappelli

indice

Il gioco dei cappelli

Dal *The New York Times* del 10 aprile 2001

Why Mathematicians Now Care About Their Hat Color

By SARA ROBINSON
Published: April 10, 2001

It takes a particularly clever puzzle to stump a mind accustomed to performing mental gymnastics.

So it's no ordinary puzzle that's spreading through networks of mathematicians like a juicy bit of gossip. Known as "the hat problem" in its most popular incarnation, this seemingly simple puzzle is consuming brain cycles at universities and research labs across the country and has become a vibrant topic of discussion on the Internet.

The reason this problem is so captivating, mathematicians say, is that it is not just a recreational puzzle to be solved and put away.

Rather, it has deep and unexpected connections to coding theory, an active area of mathematical research with broad applications in telecommunications and computer science.

http://www.nytimes.com/2001/04/10/science/why-mathematicians-now-care-about-their-hat-color.html

Descrizione del gioco

Vi è una squadra costituita da n giocatori $A_1, A_2, \ldots, A_n$.

1. Sulla testa di ogni giocatore viene posto un cappello di colore rosso o blu, in modo casuale e in modo che ciascun giocatore possa vedere il colore del cappello degli altri ma non del proprio.
2. Ciascun giocatore scrive su un foglio quello che pensa sia il colore del proprio cappello oppure passa (cioè consegna il foglio bianco), senza comunicare con gli altri e senza conoscere il contenuto del foglio da loro consegnato.
3. La squadra vince se non tutti i giocatori hanno passato e coloro che hanno scritto un colore hanno indovinato quello del proprio cappello.
4. Prima di iniziare il gioco $A_1, A_2, \ldots, A_n$ possono accordarsi su una strategia da seguire.

Descrizione del gioco

Vi è una squadra costituita da n giocatori $A_1, A_2, \ldots, A_n$.

1. Sulla testa di ogni giocatore viene posto un cappello di colore rosso o blu, in modo casuale e in modo che ciascun giocatore possa vedere il colore del cappello degli altri ma non del proprio.
2. Ciascun giocatore scrive su un foglio quello che pensa sia il colore del proprio cappello oppure passa (cioè consegna il foglio bianco), senza comunicare con gli altri e senza conoscere il contenuto del foglio da loro consegnato.
3. La squadra vince se non tutti i giocatori hanno passato e coloro che hanno scritto un colore hanno indovinato quello del proprio cappello.
4. Prima di iniziare il gioco $A_1, A_2, \ldots, A_n$ possono accordarsi su una strategia da seguire.

Descrizione del gioco

Vi è una squadra costituita da n giocatori $A_1, A_2, \ldots, A_n$.

1. Sulla testa di ogni giocatore viene posto un cappello di colore rosso o blu, in modo casuale e in modo che ciascun giocatore possa vedere il colore del cappello degli altri ma non del proprio.
2. Ciascun giocatore scrive su un foglio quello che pensa sia il colore del proprio cappello oppure passa (cioè consegna il foglio bianco), senza comunicare con gli altri e senza conoscere il contenuto del foglio da loro consegnato.
3. La squadra vince se non tutti i giocatori hanno passato e coloro che hanno scritto un colore hanno indovinato quello del proprio cappello.
4. Prima di iniziare il gioco $A_1, A_2, \ldots, A_n$ possono accordarsi su una strategia da seguire.

Descrizione del gioco

Vi è una squadra costituita da n giocatori $A_1, A_2, \ldots, A_n$.

1. Sulla testa di ogni giocatore viene posto un cappello di colore rosso o blu, in modo casuale e in modo che ciascun giocatore possa vedere il colore del cappello degli altri ma non del proprio.
2. Ciascun giocatore scrive su un foglio quello che pensa sia il colore del proprio cappello oppure passa (cioè consegna il foglio bianco), senza comunicare con gli altri e senza conoscere il contenuto del foglio da loro consegnato.
3. La squadra vince se non tutti i giocatori hanno passato e coloro che hanno scritto un colore hanno indovinato quello del proprio cappello.
4. Prima di iniziare il gioco $A_1, A_2, \ldots, A_n$ possono accordarsi su una strategia da seguire.

Vi è una squadra costituita da n giocatori $\mathbf{A_1}, \mathbf{A_2}, \ldots, \mathbf{A_n}$.

1. Sulla testa di ogni giocatore viene posto un cappello di colore rosso o blu, in modo casuale e in modo che ciascun giocatore possa vedere il colore del cappello degli altri ma non del proprio.
2. Ciascun giocatore scrive su un foglio quello che pensa sia il colore del proprio cappello oppure passa (cioè consegna il foglio bianco), senza comunicare con gli altri e senza conoscere il contenuto del foglio da loro consegnato.
3. La squadra vince se non tutti i giocatori hanno passato e coloro che hanno scritto un colore hanno indovinato quello del proprio cappello.
4. Prima di iniziare il gioco $\mathbf{A_1}, \mathbf{A_2}, \ldots, \mathbf{A_n}$ possono accordarsi su una strategia da seguire.

Alla ricerca di una strategia

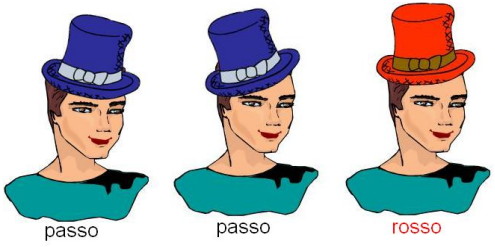
- Non esiste un modo per sapere con certezza qual è il colore del proprio cappello: *i colori dei cappelli degli altri, che un giocatore vede, sono indipendenti dal colore del proprio cappello.*
- Esiste una strategia che permette di vincere il gioco nel 50% dei casi: *un giocatore, per esempio* $\mathbf{A_1}$*, scrive a caso rosso o blu e tutti gli altri passano.*

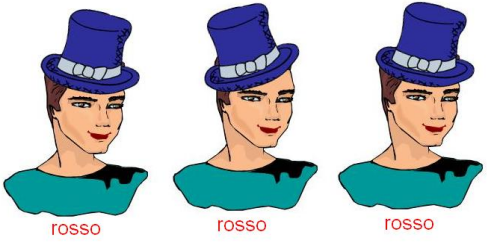
PROBLEMA 341

Trovare una strategia con cui la probabilità di vincere il gioco sia maggiore di $\frac{1}{2}$.

Esempio: il caso di tre giocatori
“Scommettiamo” sulle configurazioni con cappelli di colore diverso

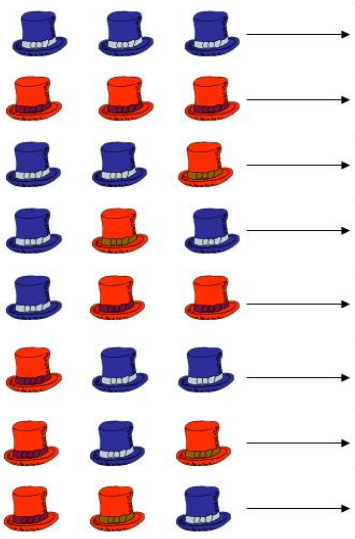
Se un giocatore vede due cappelli dello stesso colore, scrive sul foglio l’altro colore e, nel caso contrario, passa.





Esempio: il caso di tre giocatori

La strategia proposta è vincente 3 volte su quattro!



rosso	rosso	rosso
blu	blu	blu
passo	passo	rosso
passo	rosso	passo
blu	passo	passo
rosso	passo	passo
passo	blu	passo
passo	passo	blu

si perde in 2 casi

si vince in 6 casi

Posto $n = 2^m - 1$, il codice di Hamming $Ham(m, 2)$ è un $[n, n-m, 3]-$codice binario lineare perfetto e, pertanto, ha le seguenti proprietà:

- $Ham(m, 2)$ ha ordine 2^{n-m} e due sue parole distinte hanno distanza (di Hamming) maggiore di 2, cioè differiscono in almeno 3 posizioni;
- le sfere di Hamming di centro le parole di $Ham(m, 2)$ e raggio 1 costituiscono una partizione dell'insieme Z_2^n di tutte le parole binarie di lunghezza n

  o, equivalentemente,

  per ogni parola $\mathbf{b} \in Z_2^n \setminus Ham(m, q)$, esiste un'unica parola $\mathbf{a} \in Ham(m, q)$ a distanza 1 da $\mathbf{b}$.

OSSERVAZIONE 342

Queste proprietà di $Ham(m, 2)$, come vedremo, permettono di generalizzare al caso di $n = 2^m - 1$ giocatori la strategia adottata per 3 giocatori (si noti che $Ham(2, 2) = \{000\,,\ 111\}$). Sorprendentemente, la strategia che così si ottiene risulta vincente in $2^m - 1$ casi su 2^m.

Nel seguito supporremo $n = 2^m - 1$.

Denoteremo con $\mathcal{D}$ l'insieme delle 2^n possibili distribuzioni dei cappelli sulle teste dei giocatori $\mathbf{A_1}, \mathbf{A_2}, \ldots, \mathbf{A_n}$.

Denoteremo, inoltre, con 0 e 1 rispettivamente i colori rosso e blu.

Allora ogni distribuzione di cappelli $\mathbf{a} \in \mathcal{D}$ può identificarsi con la parola binaria $(a_1, a_2, \ldots, a_n) \in Z_2^n$ di lunghezza n, ove a_i è il colore del cappello del giocatore $\mathbf{A_i}$ nella distribuzione $\mathbf{a}$.

Una notazione

Per ogni $i = 1, 2, \ldots, n$ e ogni distribuzione di cappelli $\mathbf{a} \in Z_2^n$, denotiamo con $C_i(\mathbf{a})$ la parola di lunghezza $n-1$ che si ottiene cancellando da $\mathbf{a}$ la sua $i-$esima componente:

$$C_i(\mathbf{a}) = (a_1, a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n).$$

OSSERVAZIONE 343

1. Nel corso del gioco, la parola $C_i(\mathbf{a})$ può interpretarsi come ciò che vede il giocatore $\mathbf{A_i}$ quando si sceglie la distribuzione di cappelli $\mathbf{a}$.
2. Per ogni parola binaria $\mathbf{b}$ di lunghezza $n-1$ e per ogni $i = 1, 2, \ldots, n$, esistono esattamente due parole binarie $\mathbf{b}_i^-, \mathbf{b}_i^+ \in Z_2^n$ tali che $C_i(\mathbf{b}_i^-) = C_i(\mathbf{b}_i^+) = \mathbf{b}$:

$$\mathbf{b}_i^- = (b_1, \ldots, b_{i-1}, 0, b_i, \ldots, b_{n-1}), \ \mathbf{b}_i^+ = (b_1, \ldots, b_{i-1}, 1, b_i, \ldots, b_{n-1}).$$

(Notiamo che la distanza tra $\mathbf{b}_i^-$ e $\mathbf{b}_i^+$ è pari ad 1.)

Osservazione

Siano $\mathbf{b} = (b_1, b_2, \ldots, b_{n-1})$ una parola binaria di lunghezza $n-1$ e, per ogni $i = 1, 2, \ldots, n$,

$$\mathbf{b}_i^- = (b_1, \ldots, b_{i-1}, 0, b_i, \ldots, b_{n-1}),$$

$$\mathbf{b}_i^+ = (b_1, \ldots, b_{i-1}, 1, b_i, \ldots, b_{n-1})$$

le uniche due parole binarie tali che $C_i(\mathbf{b}_i^-) = C_i(\mathbf{b}_i^+) = \mathbf{b}$.
Allora $\mathbf{b}_i^-$ e $\mathbf{b}_i^+$, avendo tra loro distanza 1, non possono entrambi appartenere a $Ham(m, 2)$ e, quindi, si verifica una soltanto delle seguenti eventualità:

1. $\mathbf{b}_i^- \notin Ham(m, 2)$, $\mathbf{b}_i^+ \in Ham(m, 2)$;
2. $\mathbf{b}_i^- \in Ham(m, 2)$, $\mathbf{b}_i^+ \notin Ham(m, 2)$;
3. $\mathbf{b}_i^- \notin Ham(m, 2)$, $\mathbf{b}_i^+ \notin Ham(m, 2)$.

La strategia di Hamming

Assegnata una distribuzione di cappelli $\mathbf{b} = (b_1, b_2, \ldots, b_n) \in Z_2^n$, per ogni $i = 1, 2, \ldots, n$, il giocatore $\mathbf{A_i}$ vede la parola

$$C_i(\mathbf{b}) = (b_1, b_2, \ldots, b_{i-1}, b_{i+1}, \ldots, b_n) \in Z_2^{n-1}$$

e sceglie

1. il *colore rosso* se
   $C_i(\mathbf{b})_i^+ = (b_1, b_2, \ldots, b_{i-1}, 1, b_{i+1}, \ldots, b_n) \in Ham(m, 2)$,
2. il *colore blu* se
   $C_i(\mathbf{b})_i^- = (b_1, b_2, \ldots, b_{i-1}, 0, b_{i+1}, \ldots, b_n) \in Ham(m, 2)$,
3. di *passare* se $C_i(\mathbf{b})_i^+$ e $C_i(\mathbf{b})_i^-$ non appartengono a $Ham(m, 2)$.

La strategia descritta sarà detta strategia di Hamming e chiaramente consiste nello "scommettere" sull'eventualità che $\mathbf{b}$ non appartenga ad $Ham(m, 2)$.

La strategia di Hamming è perdente se la distribuzione di cappelli assegnata $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ appartiene a $Ham(m,2)$.

In queste ipotesi, per ogni $i = 1, 2, \ldots, n$, una delle due parole $C_i(\mathbf{b})_i^+$, $C_i(\mathbf{b})_i^-$ è uguale a $\mathbf{b}$ e l'altra non appartiene a $Ham(m,2)$.

Allora ogni giocatore $\mathbf{A_i}$, scegliendo
- il colore rosso se $\mathbf{b} = C_i(\mathbf{b})_i^+ \in Ham(m,2)$ o
- il colore blu se $\mathbf{b} = C_i(\mathbf{b})_i^- \in Ham(m,2)$,

sceglie il colore sbagliato.

La strategia di Hamming è vincente se la distribuzione di cappelli assegnata $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ non appartiene a $Ham(m,2)$.

In queste ipotesi, sia $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ l'unica parola di $Ham(m,q)$ a distanza 1 da $\mathbf{b}$ e supponiamo che $\mathbf{a}$ e $\mathbf{b}$ differiscono nella $k-$esima posizione, cioè $a_k \neq b_k$ e

$$(a_1, a_2, \ldots, a_{k-1}, a_{k+1}, \ldots, a_n) = (b_1, b_2, \ldots, b_{k-1}, b_{k+1}, \ldots, b_n).$$

Allora, una delle due parole $C_k(\mathbf{b})_k^+$, $C_k(\mathbf{b})_k^-$ è uguale a $\mathbf{b}$ e l'altra ad $\mathbf{a} \in Ham(m,2)$. Così $\mathbf{A_k}$, scrivendo rosso se $\mathbf{a} = C_k(\mathbf{b})_j^+$ o blu se $\mathbf{a} = C_k(\mathbf{b})_j^-$, sceglie il colore giusto.
Inoltre, ogni giocatore $\mathbf{A_i}$, con $i \neq k$, passa perché $C_i(\mathbf{b})_i^+$ e $C_i(\mathbf{b})_i^-$ non appartengono a $Ham(m,2)$.

Riassumendo, abbiamo che la strategia di Hamming

- è perdente se la distribuzione dei cappelli appartiene ad $Ham(m, q)$;
- è vincente se la distribuzione dei cappelli non appartiene ad $Ham(m, q)$.

CONCLUSIONE 344

La probabilità di vincita al gioco dei cappelli con la strategia di Hamming è

$$\frac{|Z_2^n \setminus Ham(m, 2)|}{|Z_2^n|} = \frac{2^n - 2^{n-m}}{2^n} = \frac{2^m - 1}{2^m} .$$

In altre parole, la strategia di Hamming risulta vincente in $2^m - 1$ casi su 2^m.

CODICI CICLICI

1. Richiami sugli anelli di polinomi

indice

Denotiamo con $F[x]$ l'anello (commutativo unitario) dei polinomi nell'indeterminata x a coefficienti in un campo F. Un elemento $f \in F[x]$ è del tipo

$$f(x) = a_o + a_1 x + a_2 x^2 + \cdots + a_n x^n, \ a_o, a_1, \ldots, a_n \in F.$$

Se $n \neq 0$, l'intero n è il grado di f e si denota con $deg\, f$.
Al polinomio nullo non si attribuisce alcun grado.

OSSERVAZIONE 345

Gli elementi invertibili di $F[x]$ sono tutti e soli quelli non nulli del campo F (costanti non nulle).

RISULTATO (Divisione euclidea) 346

Se $f, g \in F[x]$, con $g \neq 0$, esiste un'unica coppia di polinomi (q, r) tali che

$$f = qg + r\,, \quad \text{con} \quad r = 0 \ \text{ o } \deg r < \deg g$$

(q ed r si chiamano, rispettivamente, *quoziente* e *resto* della divisione fra f e g e si calcolano col ben noto algoritmo di Euclide).

CONVENZIONE 347

Se f, g sono due polinomi, la notazione $g \mid f$ indica che g divide f, cioè che esiste un polinomio c tale che $f = cg$. In queste ipotesi la divisione euclidea tra f e g ha resto nullo.

RISULTATO 348

$F[x]$ è un anello principale; ogni suo ideale J, quindi, è principale, cioè contiene qualche polinomio $c(x) = c_0 + c_1 x + \cdots + c_{m-1} x^{m-1} + c_m x^m$ che lo genera:

$$J = (c(x)) = \{f(x)c(x) \ : \ f(x) \in F_q[x]\} .$$

RISULTATO 349

I generatori di un ideale J di $F[x]$ sono tutti e soli i polinomi di grado minimo in J; questi differiscono tra loro per una costante moltiplicativa non nulla e, tra essi, ve ne è uno solo monico $m = m(x)$ (il *polinomio minimo* di J). Risulta, quindi,

$$J = (m(x)) = \{h(x)m(x) \ : \ h(x) \in F[x]\}$$

e i generatori di J sono tutti e soli i polinomi del tipo $am(x)$, con $a \in F^*$.

RISULTATO 350

Se $J_1 = (c_1(x))$ e $J_2 = (c_2(x))$ sono ideali di $F_q[x]$, risulta

RISULTATO 351

Sia J un ideale di $F[x]$.

- La relazione

$$f(x) \sim g(x) \Leftrightarrow f(x) - g(x) \in J$$

è di equivalenza in $F[x]$ e le sue classi di equivalenza sono i *laterali* di J in $F[x]$.

- Il laterale $[f]_J$ di J individuato dal polinomio $f(x)$ è dato da

$$[f]_J = f(x) + J = \{f(x) + h(x) \ : \ h(x) \in J\}$$

e risulta

$$f(x) + J = J \Leftrightarrow f(x) \in J.$$

OSSERVAZIONE 352

Sull'insieme dei laterali di J in $F[x]$, che si denota con $F[x]/J$, sono ben definite le seguenti operazioni di *addizione* e *moltiplicazione*:

$$[f]_J + [g]_J = [f+g]_J \ , \ [f]_J[g]_J = [fg]_J \, .$$

RISULTATO 353

Sia J un ideale di $F[x]$.

- La struttura algebrica

$$F[x]/J = (F[x]/J, +, \cdot)$$

è un dominio d'integrità (*l'anello quoziente* di $F[x]$ rispetto all'ideale J).

- In $F[x]/J$ si ha:

$$0 = [0]_J = 0 + J = J \ , \quad 1 = [1]_J = 1 + J \ , \quad -[f]_J = [-f]_J.$$

OSSERVAZIONE 354

Risulta $$F[x]/F[x] = \{0\} \ , \ F[x]/(0) = F[x].$$

RISULTATO 355

Se J è un ideale di $F[x]$, gli ideali H dell'anello quoziente $F[x]/J$ sono tutti e soli quelli del tipo I/J, ove I è un ideale di $F[x]$ contenente J.

DEFINIZIONE 356

Un ideale J di $F[x]$ si dice *massimale* se è proprio, cioè diverso da $F[x]$, e non è propriamente contenuto in alcun ideale proprio di $F[x]$.

RISULTATO 357

Un anello commutativo unitario A è un campo se, e solo se, i suoi unici ideali sono l'ideale nullo e A.

RISULTATO 358

Sia J un ideale di $F[x]$. Allora J è un ideale massimale se, e solo se, il quoziente $F[x]/J$ è un campo.

Radici di un polinomio

DEFINIZIONE 359

Un'equazione del tipo $f(x) = 0$, $f \in F[x]$ con $deg(f) = n$, si chiama *equazione algebrica di grado n* e un elemento $c \in A$ si dice *radice* o *zero* di f se risulta $f(c) = 0$.

RISULTATO 360

Siano $f \in F[x]$ un polinomio di grado n e c un elemento di F. Allora esiste un unico polinomio $q \in F[x]$ tale che

$$f = (x - c)q + f(c) \quad \text{(teorema del resto)}.$$

Ne segue che:

- (teorema di Ruffini) c è una radice di f se, e solo se, $(x - c)$ divide f.
- f possiede al più n radici in F.

DEFINIZIONE 361

Un polinomio $f \in F[x]$ di grado positivo si dice *irriducibile in* $F[x]$, o *irriducibile su* F se

$$f = gh\,, \quad g, h \in F[x]\,, \deg h > 0 \quad \Rightarrow \quad g \text{ costante}\,.$$

Se f non è irriducibile, si dice *riducibile*.

RISULTATO 362

Un polinomio $f \in F[x]$ di grado positivo è irriducibile su F se, e solo se,

$$f \mid gh \text{ con } g, h \in F[x] \quad \Rightarrow \quad f \mid g \text{ o } f \mid h.$$

RISULTATO 363

Ogni polinomio di grado positivo a coefficienti in F è prodotto di polinomi irriducibili su F.

OSSERVAZIONE 364

Il polinomio x è irriducibile in $F[x]$. Ogni polinomio di primo grado a coefficienti in F ha una radice in F ed è ivi irriducibile.

RISULTATO 365

Sia $f \in F[x]$ un polinomio irriducibile su F di grado maggiore di 1. Allora F non contiene radici di f.

RISULTATO 366

Sia $f \in K[x]$ un polinomio di grado 2 o 3 e si supponga che f non abbia radici in F. Allora f è irriducibile su F.

RISULTATO 367

L'ideale (f) generato da $f \in F[x]$ è massimale in $F[x]$ se, e soltanto se, f è irriducibile su F. Ne segue che l'anello quoziente $F[x]/(f)$ è un campo se, e soltanto se, f è irriducibile.

ESERCIZIO 368

Provare che un polinomio $f \in F[x]$ di grado 2 o 3 è riducibile su F se, e solo se, f ha una radice in F.

Proprietà di $F_q[x]/(x^n - 1)$

Sia $(x^n - 1)$ l'ideale di $F_q[x]$ generato dal polinomio $x^n - 1$, cioè

$$(x^n - 1) = \{h(x)(x^n - 1) \ : \ h(x) \in F_q[x]\},$$

e denotiamo con $Pol_q[n, x] = F_q[x]/(x^n - 1)$ l'anello quoziente di $F_q[x]$ rispetto all'ideale $(x^n - 1)$.

- Ogni elemento di $Pol_q[n, x]$ è un laterale dell'ideale $(x^n - 1)$, e quindi è un insieme del tipo

$$f(x) + (x^n - 1) \ , \ \text{con } f(x) \in F_q[x] \ .$$

- Due polinomi $f(x), g(x)$ definiscono lo stesso laterale di $(x^n - 1)$ se, e solo se,

$$f(x) - g(x) \in (x^n - 1) \ ,$$

cioè, se, e solo se, esiste $h(x) \in F_q[x]$ tale che

$$f(x) - g(x) = h(x)(x^n - 1).$$

- Ogni ideale di $Pol_q[n, x]$ è del tipo $(f(x))/(x^n - 1)$, ove $f(x) \in F_q[x]$ divide $x^n - 1$.

Proprietà di $F_q[x]/(x^n - 1)$

- Per ogni $f(x) \in F_q[x]$, risulta

$$f(x) + (x^n - 1) = r(x) + (x^n - 1),$$

ove $r(x)$ è il resto della divisione euclidea tra $f(x)$ e $x^n - 1$. [**N.B.** $r(x)$ si calcola ponendo $x^n = 1$ in $f(x)$]
Per tale resto si usa la notazione

$$r(x) = f(x)\, mod(x^n - 1)$$

e risulta

$$f(x) = f(x)\, mod(x^n - 1) \Leftrightarrow degf(x) < n \ o \ f = 0.$$

- Due polinomi appartengono ad uno stesso laterale di $(x^n - 1)$ se, e solo se, hanno lo stesso resto della divisione per $x^n - 1$.
- Ogni laterale proprio H dell'ideale $(x^n - 1)$ contiene un unico polinomio $r_H(x)$ di grado minore di n e, per ogni $f(x) \in H$, risulta

$$r_H(x) = f(x)\, mod(x^n - 1).$$

Se $f(x), g(x) \in F_q[x]$ poniamo:

$$f(x) +_n g(x) = (f(x) + g(x)) \, mod(x^n - 1) \ ,$$

$$f(x) \cdot_n g(x) = f(x)g(x) \, mod(x^n - 1) \ .$$

OSSERVAZIONE 369

Sia $F_q[n, x]$ l'insieme dei polinomi di $F_q[x]$ di grado minore di n e del polinomio nullo. Su tale insieme l'ordinaria operazione di addizione in $F_q[x]$ e l'operazione $+_n$ coincidono.

PROPOSIZIONE 370

La struttura algebrica $F_q[n, x] = (F_q[n, x], +, \cdot_n)$ è un anello commutativo unitario. La funzione

$$f(x) \in F_q[x] \rightarrow f(x) \, mod(x^n - 1) \in F_q[n, x],$$

è un epimorfismo di anelli unitari il cui nucleo è l'ideale $(x^n - 1)$.

Ne segue che gli anelli $\frac{F_q[x]}{(x^n-1)}$ e $F_q[n, x]$ sono isomorfi, in simboli

$$Pol_q[n, x] = \frac{F_q[x]}{(x^n - 1)} \sim F_q[n, x]. \tag{49}$$

OSSERVAZIONE 371

La relazione

$$Pol_q[n, x] = \frac{F_q[x]}{(x^n - 1)} \sim F_q[n, x]$$

permette di identificare l'anello quoziente $Pol_q[n, x]$ con l'anello $F_q[n, x]$. Questo significa che, per operare nell'anello $F_q[x]/(x^n - 1)$, possiamo prima identificarlo con $F_q[n, x]$ e operare, poi, in $F_q[x]$ ponendo $x^n = 1$.

CONVENZIONE 372

Nel seguito, in assenza di possibilità di equivoci, useremo il simbolo standard per l'operazione di moltiplicazione in $F_q[n, x]$ in luogo di $''\cdot_n''$.

- $F_q[x]$, rispetto all'addizione fra polinomi e alla moltiplicazione di un polinomio per uno scalare, è uno spazio vettoriale di dimensione infinita su F_q.
- $F_q[n, x]$, rispetto alle suddette operazioni, è un sottospazio vettoriale di $F_q[x]$ di dimensione n. Esso è, quindi, isomorfo a F_q^n e una sua base (canonica) è data da

$$\{1, x, x^2, \ldots, x^{n-1}\}.$$

- $F_q[n, x]$ non è un sottoanello di $F_q[x]$.

Convenzione

Per lo studio di alcune classi di codici lineari, come per esempio i codici ciclici, spesso conviene utilizzare $F_q[n, x]$ come modello di spazio vettoriale di dimensione n su F_q, in luogo di F_q^n.

2. Codici ciclici

indice

Cambio di notazione

Nel seguito una parola $\mathbf{a} \in F_q^n$ sarà denotata con $a_0 a_1 ... a_{n-1}$ invece che con $a_1 a_2 ... a_n$. Con questa notazione, posto

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}, \tag{50}$$

la funzione

$$\mathbf{a} \in F_q^n \rightarrow a(x) \in F_q[x]$$

è iniettiva e, quindi, ogni parola

$$\mathbf{a} = (a_0, a_1, ..., a_{n-1}) \in F_q^n$$

può identificarsi col corrispondente polinomio di $a(x) \in F_q[x]$.

Osservazione

Tenendo presente che
- i polinomi che si ottengono nella (50) sono tutti e soli quelli di grado minore di n,
- ogni laterale proprio dell'ideale (x^n-1) di $F_q[x]$ generato da x^n-1 contiene un unico polinomio di grado minore di n,

la funzione

$$\mathbf{a} \in F_q^n \to a(x) \in F_q[n,x] \tag{51}$$

è biunivoca e, quindi, induce una biiezione fra F_q^n e l'anello quoziente

$$Pol_q[n,x] = F_q[x]/(x^n-1) \sim F_q[n,x].$$

In questo modo, ogni parola $\mathbf{a} \in F_q^n$ viene sostanzialmente identificata col resto della divisione di $a(x)$ per x^n-1.

CONVENZIONE 373

Per ogni sottoinsieme S di F_q^n, denoteremo con $S(x)$ il corrispondente sottoinsieme in $Pol_q[n,x]$ mediante la (51).

DEFINIZIONE 374

Un $[n,k]-$codice C su F_q si dice *ciclico* se verifica la seguente proprietà

$$(a_0, a_1, ..., a_{n-2}, a_{n-1}) \in C \;\Rightarrow\; (a_{n-1}, a_0, ..., a_{n-3}, a_{n-2}) \in C. \qquad (52)$$

ESEMPI 375

- I codici di ripetizione $q-$ari sono banalmente ciclici.
- Il codice binario

$$C = \{000\,,\, 110\,,\, 101\,,\, 011\}$$

è ciclico. Osserviamo che risulta

$$C(x) = \{0\,,\, 1+x\,,\, 1+x^2\,,\, x+x^2\} \subseteq Pol_2[3,x].$$

Osservazione

Se si riguarda $Pol_q[n,x] \sim F_q[n,x]$ come spazio vettoriale su F_q, la biiezione

$$\mathbf{a} \in F_q^n \rightarrow a(x) \in Pol_q[n,x]$$

è chiaramente un isomorfismo di spazi vettoriali e, $C(x)$ è un sottospazio vettoriale di $Pol_q[n,x]$. Con queste posizioni si ha subito che la (52)

$$(a_0, a_1, ..., a_{n-2}, a_{n-1}) \in C \;\Rightarrow\; (a_{n-1}, a_0, ..., a_{n-3}, a_{n-2}) \in C.$$

equivale a

$$a(x) \in C(x) \Rightarrow xa(x) \in C(x). \qquad (53)$$

PROBLEMA 376

I codici lineari di lunghezza n su F_q corrispondono biunivocamente ai sottospazi vettoriali di $Pol_q[n, x]$.
Ovviamente non tutti questi codici sono ciclici.
Ci chiediamo: cosa corrisponde ai codici ciclici in $Pol_q[n, x]$?

OSSERVAZIONE 377

Gli ideali dell'anello $Pol_q[n, x]$ sono anche sottospazi vettoriali; in generale, non è vero il contrario.

PROPOSIZIONE 378

Un codice lineare C su F_q è ciclico se, e soltanto se, $C(x)$ è un ideale di $Pol_q[n, x]$.

DIMOSTRAZIONE 379

Identifichiamo $Pol_q[n, x]$ con $F_q[n, x]$ e supponiamo che C sia ciclico. Allora $C(x)$, essendo lineare, è sottospazio vettoriale di $F_q[n, x]$. Per ogni $a(x) \in C(x)$ e $b(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$ in $F_q[n, x]$, risulta

$$b(x)a(x) = b_0 a(x) + b_1 xa(x) + \cdots + b_{n-1}x^{n-1}a(x).$$

Ne segue che $b(x)a(x)$ è in $C(x)$ perchè, in forza della (53), $x^s a(x)$ è in $C(x)$, per ogni intero non negativo s.
Supponiamo, ora, che $C(x)$ sia un ideale di $F_q[n, x]$. Allora C è sottospazio vettoriale di F_q^n e, per ogni parola $\mathbf{a} \in C$, $xa(x)$ è un elemento di $C(x)$; cioè C è ciclico.

Ogni ideale $C(x)$ di $Pol_q[n, x]$ è un quoziente $J/(x^n - 1)$, con $J = (c(x))$ ideale di $F_q[x]$ contenente l'ideale $(x^n - 1)$, così

$$J/(x^n - 1) \text{ è un ideale di } Pol_q[n, x] \Leftrightarrow c(x) \mid (x^n - 1).$$

Ogni generatore $c(x)$ di J, che può identificarsi con un generatore di $C(x)$, si chiama *polinomio generatore* di C e gli ideali di $Pol_q[n, x]$ sono in corrispondenza biunivoca con i divisori del polinomio $x^n - 1$ a meno di una costante moltiplicativa non nulla.

ESEMPIO 380

È possibile provare che i codici di Golay $\mathcal{G}_{23}$ e $\mathcal{G}_{11}$ sono ciclici e, per esempio, $x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$ e $x^5 - x^3 + x^2 - x - 1$ sono dei polinomi generatori, rispettivamente.

Il numero dei codici ciclici

- Il numero degli $[n, k]-$codici ciclici su F_q è uguale al numero dei polinomi di $F_q[x]$ che dividono $x^n - 1$, a meno di una costante moltiplicativa non nulla.

- Se $x^n - 1$ possiede s fattori irriducibili distinti (a meno di una costante moltiplicativa non nulla) in $F_q[x]$, il numero degli $[n, k]-$codici ciclici su F_q è 2^s, in tale numero essendo compresi anche il codice nullo $\{\mathbf{0}\}$ e F_q^n.

Esempio

Il polinomio $x^4 - 1 \in F_3[x]$, ha la seguente decomposizione in fattori irriducibili

$$x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$$

e quindi abbiamo otto polinomi a coefficienti in F_3 che dividono $x^4 - 1$:

$$1\ ,\ x - 1\ ,\ x + 1\ ,\ x^2 + 1\ ,\ (x - 1)(x + 1)\ ,$$

$$(x - 1)(x^2 + 1)\ ,\ (x + 1)(x^2 + 1)\ ,\ x^4 - 1\ .$$

Esistono, pertanto, otto codici ciclici di lunghezza 4 su F_3.

PROPOSIZIONE 381

Sia C un $[n,k]-$codice ciclico su F_q con polinomio generatore di grado m

$$c(x) = c_0 + c_1 x + \cdots + c_{m-1}x^{m-1} + c_m x^m.$$

Allora la matrice di tipo $(n-m) \times n$

$$G_c = \begin{bmatrix} c_0 & c_1 & \cdots & c_m & & 0 \\ & c_0 & c_1 & \cdots & c_m & \\ & & \ddots & & & \\ & 0 & & c_0 & \cdots & c_{m-1} & c_m \end{bmatrix}$$

è una matrice generatrice di C e, di conseguenza, è $k = n - m$.

- Le righe di G_c sono indipendenti e sono parole di C perchè i polinomi corrispondenti sono

$$c(x), xc(x), ..., x^{n-m-1}c(x) \text{ e } \mathbf{c} \in C.$$

- Se $\mathbf{a} \in C \Rightarrow a(x) \in C(x) \Rightarrow$ esiste un polinomio $q(x)$ di grado minore di $n-m$ tale che

$$a(x) = q(x)c(x). \tag{54}$$

Essendo i gradi di $a(x), q(x), c(x)$ non superiori ad n, l'uguaglianza precedente in $Pol_q[n, x]$ è un'uguaglianza anche in $F_q[x]$ e così abbiamo

$$a(x) = q_0 c(x) + q_1 xc(x) + \cdots + q_{n-m-1}x^{n-m-1}c(x),$$

cioè $\mathbf{a}$ è combinazione lineare delle righe di G_c.

DEFINIZIONE 382

Se $c(x)$ è un polinomio generatore di un codice ciclico C, cioè

$$C(x) = (c(x))/(x^n - 1), \text{ con } c(x) \mid x^n - 1 ,$$

il polinomio $h(x) \in F_q[x]$, definito da $x^n - 1 = c(x)h(x)$, prende il nome di *polinomio di controllo* di C.

ESEMPIO 383

Un codice ciclico di lunghezza 4 su F_3 è generato da uno dei seguenti polinomi:

$$1 , \quad x-1 \ , \ x+1 \ , \ x^2+1 \ , \ (x-1)(x+1) ,$$

$$(x-1)(x^2+1) \ , \ (x+1)(x^2+1) \ , \ x^4-1 .$$

I rispettivi polinomi di controllo sono:

$$x^4-1 , \quad (x+1)(x^2+1) \ , \ (x-1)(x^2+1) ,$$

$$(x-1)(x+1), \quad x^2+1 , \ x+1 , \ x-1 , \quad 1 .$$

Proprietà delle parole di un codice ciclico

PROPOSIZIONE 384

Sia C un $[n,k]-$codice ciclico su F_q con polinomio generatore $c(x)$ di grado m e relativo polinomio di controllo $h(x)$. Allora una parola $\mathbf{a} \in F_q^n$ appartiene al codice C se, e soltanto se, risulta $a(x)h(x) = 0$ in $Pol_q[n,x]$.

DIMOSTRAZIONE 385

- Se $\mathbf{a} \in C \Rightarrow a(x) \in C(x) \Rightarrow$ esiste un polinomio $q(x)$ di grado minore di $n-m$ tale che $a(x) = q(x)c(x)$.
  Ne segue che: $a(x)h(x) = q(x)c(x)h(x) = (x^n-1)q(x) = 0$ in $Pol_q[n,x]$.
- Ora, per $a(x) \in F_q[x]$, con $deg(a) < n$, sia $a(x)h(x) = 0$ in $Pol_q[n,x]$.
  Allora esiste un polinomio $g(x) \in F_q[x]$ tale che, in $F_q[x]$, risulta

$$a(x)h(x) = g(x)(x^n-1) = g(x)c(x)h(x).$$

Ne segue che $a(x) = g(x)c(x)$, cioè $a(x) \in C(x)$.

Reciproco del polinomio di controllo

OSSERVAZIONE 386

Un polinomio di controllo di C è anche polinomio generatore di un codice avente la stessa dimensione di $C^{\perp}$. Tale codice non coincide con $C^{\perp}$ perchè la relazione $a(x)h(x) = 0$ in $Pol_q[n, x]$ non equivale all'annullarsi del prodotto scalare **ah**.

PROPOSIZIONE 387

Sia C un $[n, k]-$codice lineare ciclico su F_q con polinomio di controllo

$$h(x) = h_0 + h_1 x + \cdots + h_{k-1}x^{k-1} + h_k x^k.$$

Allora la matrice di tipo $(n-k) \times n$

$$H_h = \begin{bmatrix} h_k & h_{k-1} & \cdots & h_0 & & & & & \\ 0 & h_k & h_{k-1} & \cdots & h_0 & & 0 & & \\ & & & & \ddots & & & & \\ & & 0 & & h_k & h_{k-1} & \cdots & h_0 & 0 \\ & & & & & h_k & h_{k-1} & \cdots & h_0 \end{bmatrix}$$

è una matrice controllo di parità di C. Inoltre, $C^{\perp}$ è ciclico e il polinomio (reciproco di $h(x)$)

$$\overline{h}(x) = h_k + h_{k-1}x + h_{k-2}x^2 + \cdots + h_1 x^{k-1} + h_0$$

è un suo polinomio generatore.

Esempio

Il polinomio

$$c(x) = 1 + x + x^3 \in Z_2[x]$$

divide $x^7 + 1$ e, quindi, è polinomio generatore di un cocice ciclico binario C di lunghezza 7 e dimensione $4 (= 7 - 3)$.
Il polinomio di controllo di C è

$$h(x) = \frac{x^7 + 1}{1 + x + x^3} = 1 + x + x^2 + x^4.$$

Una matrice generatrice G e una matrice di controllo H di C sono:

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}, \quad H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

3. Ulteriori richiami sui campi finiti

indice

RISULTATO 388

Siano $g(x) \in Z_p[x]$ un polinomio irriducibile su Z_p di grado $h > 1$ e a una radice di $g(x)$ nel suo campo di spezzamento su Z_p. Allora

$$Z_p(a) = \{m_0 + m_1 a + m_2 a^2 + \cdots + m_{h-1} a^{h-1} \ : \ m_j \in Z_p\}$$

è un campo finito d'ordine p^h (*estensione algebrica* di Z_p mediante l'aggiunta di una radice a di $g(x)$) *Ne segue che* $Z_p(a)$ *è isomorfo al campo di Galois* $GF(p^h)$ *d'ordine* $q = p^h$. *Ogni campo di Galois può ottenersi con questa costruzione.*

ESEMPIO 389

Usando il polinomio $x^2 + x + 1 \in Z_2[x]$ irriducibile su $Z_2 = \{0, 1\}$, possiamo costruire il campo di Galois d'ordine 4 :

$$GF(4) = \{0, 1, a, 1 + a\},$$

ove a ha la proprietà $a^2 + a + 1 = 0$.

ESEMPIO 390

Usando il polinomio $x^2 - x - 1 \in Z_3[x]$ irriducibile su $Z_3 = \{0, 1, -1\}$, possiamo costruire il campo di Galois d'ordine 9 :

$$GF(9) = \{0, 1, -1, a, -a, 1 + a, 1 - a, -1 + a, -1 - a\},$$

ove a ha la proprietà $a^2 - a - 1 = 0$.

Ordine degli elementi di F_q

Se F è un campo, denoteremo con F^* il suo gruppo moltiplicativo, che è costituito dai suoi elementi non nulli.
Supporremo, inoltre, costantemente $q = p^h$, p primo.

Per un elemento $a \in F_q^*$, ricordiamo che:

- l'*ordine* o *periodo* $o(a)$ è l'ordine che ha a come elemento del gruppo moltiplicativo F_q^*, cioè è il più piccolo intero positivo m tale che $a^m = 1$;
- se $a^n = 1$ per un intero n, allora $o(a)$ deve dividere n.

Elementi primitivi

RISULTATO (Teorema dell'elemento primitivo) 391

Il gruppo moltiplicativo F_q^* di F_q è ciclico, esiste cioè un elemento $\alpha \in F_q^*$ di periodo $q-1$ (*elemento primitivo* o *radice primitiva*).

OSSERVAZIONE 392

Quando si rappresentano gli elementi non nulli del campo di Galois $GF(q)$ mediante potenze di un suo elemento primitivo α è molto semplice eseguire la moltiplicazione di due elementi:

$$\alpha^i \alpha^j = \alpha^{(i+j) \bmod (q-1)}$$

ESERCIZIO 393

Trovare gli elementi primitivi del campo $GF(9)$ (cfr. 390).

DEFINIZIONE 394

Sia $GF(q)$ il campo di Galois d'ordine $q = p^h$, p primo. Detto a un elemento non nullo di $GF(q)$, l'ideale di $Z_p[x]$

$$I_a = \{f \in Z_p[x] \ : \ f(a) = 0\},$$

è non nullo perché $x^q - x$ si annulla su a. Il polinomio minimo $m_a(x)$ di I_a si chiama anche polinomio minimo di a. In altre parole $m_a(x)$ è l'unico polinomio monico tra tutti i polinomi in $Z_p[x]$ di grado minimo che si annullano su a.

Ideale generato da un polinomio minimo

PROPOSIZIONE 395

Sia $a \in GF(q)$. Il polinomio minimo $m_a(x)$ di a è irriducibile. Ne segue che l'ideale I_a è massimale in $Z_p[x]$.

DIMOSTRAZIONE 396

Se poniamo $m_a = fg$, con $f, g \in Z_p[x]$, abbiamo $m_a(a) = f(a)g(a) = 0$ e, quindi, deve essere $f(a) = 0$ oppure $g(a) = 0$. Nel primo caso, avendosi $deg(f) \leq deg(m_a)$ ed essendo m_a di grado minimo tra i polinomi di $Z_p[x]$ che si annullano su a, risulta $deg(f) = deg(m_a)$ e quindi g è una costante. Nel secondo caso si ragiona allo stesso modo e si ottiene così l'asserto.

Estensioni di Z_p in $GF(q)$

RISULTATO 397

Sia $a \in GF(q)$ e si ponga

$$Z_p[a] = \{f(a) \,:\, f \in Z_p[x]\,\}.$$

- La funzione

$$\varphi_a \,:\, f(x) \in Z_p[x] \,\rightarrow\, f(a) \in Z_p[a]$$

è un morfismo di anelli con nucleo l'ideale I_a (polinomi a coefficienti in $Z_p[x]$ che si annullano su a) e immagine $Z_p[a]$. Ne segue che $Z_p[x]/I_a$ è isomorfo a $Z_p[a]$ e, di conseguenza, $Z_p[a]$ è un campo (estensione algebrica di Z_p mediante a), sottocampo di $GF(q)$.

- $Z_p[a]$ coincide col sottocampo di $GF(q)$ generato da $Z_p \cup \{a\}$ e l'estensione $Z_p[a]/Z_p$ ha grado finito n pari al grado del polinomio minimo m_a di a. Ne segue che l'estensione $Z_p[a]$ è isomorfa a $GF(p^n)$.

Base canonica di $Z_p[a]$, $a \in GF(q)$

PROPOSIZIONE 398

Se $a \in GF(q)$ e se n è il grado del suo polinomio minimo m_a, allora

$$\{1, a, a^2, \ldots, a^{n-1}\}$$

è una base (canonica) di $Z_p[a] = GF(p^n)$ su Z_p. Ne segue che m_a divide $x^{p^n} - x$.

DIMOSTRAZIONE 399

Se così non fosse, esisterebbe un polinomio in $Z_p[x]$ di grado minore di n avente a per radice; un assurdo.

COROLLARIO 400

Siano $a \in GF(q)$ e n il grado del suo polinomio minimo m_a. Allora il campo $Z_p[a] = GF(p^n)$ è isomorfo al campo $Z_p(a)$ estensione algebrica di Z_p mediante l'aggiunta della radice a del polinomio m_a (cfr. Risultato 388).

Siano $q = p^m$ una potenza di un primo p e α un *elemento primitivo* di $GF(q)$. Allora:

- $GF(q) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$.
- Il *polinomio minimo* m_α di α, cioè il polinomio monico di grado minimo a coefficienti in Z_p che si annulla su α, ha grado m ed è irriducibile.
- L'insieme $B = \{1, \alpha, \alpha^2, ..., \alpha^{m-1}\}$ è una base di $GF(q)$ considerato come spazio vettoriale su Z_p e, quindi,

$$GF(q) = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1} \ : \ a_i \in Z_p\}.$$

4. Codici di Hamming binari

indice

Ciclicità dei codici di Hamming binari

PROPOSIZIONE 401

I codici di Hamming binari sono ciclici. Un polinomio generatore di $Ham(m, 2)$ *è il polinomio minimo* $m_\alpha(x)$ *di un qualsiasi elemento primitivo* α *del campo di Galois* $GF(2^m)$ *con* 2^m *elementi.*

DIMOSTRAZIONE 402

- Il campo di Galois $GF(2^m)$ d'ordine 2^m può essere visto come spazio vettoriale $m-$dimensionale sul sottocampo fondamentale Z_2 e, quindi, identificato con Z_2^m, qualora si fissi una sua base ordinata.
- Sia α un elemento primitivo di $GF(2^m)$, cioè un generatore del gruppo (ciclico) moltiplicativo del campo. Abbiamo

$$Z_2^m \sim GF(2^m) = \{0, 1, \alpha, \alpha^2, ..., \alpha^{2^m-2}\}$$

e l'insieme

$$B = \{1, \alpha, \alpha^2, ..., \alpha^{m-1}\}$$

è una base ordinata di Z_2^m.

DIMOSTRAZIONE (CONTINUAZIONE) 403

- Consideriamo la matrice H i cui vettori colonna sono ordinatamente le componenti in B di
$$1, \alpha, \alpha^2, ..., \alpha^{2^m-2}.$$
- Posto $n = 2^m - 1$, $Ham(m, 2)$ è il codice lineare binario avente H come matrice controllo di parità:

$$Ham(m,2) = \{\mathbf{a} = (a_0, a_1, ..., a_{n-1}) \in V(n,2) \ : \ a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} = 0\}$$

- In questa rappresentazione di $Ham(m, 2)$, il sottospazio vettoriale di $Pol_2[n, x]$ ad esso associato è un ideale, avendosi
$$Ham(m,2)(x) = \{a(x) \in Pol_2[n,x] \ : \ a(\alpha) = 0\}.$$

Ne segue che $Ham(m, 2)$ è ciclico e che un suo polinomio generatore è proprio $m_\alpha(x)$.

Decodifica con $Ham(m, 2)$

Consideriamo $Ham(m, 2)$ come codice ciclico:

$$Ham(m, 2)(x) = \{a(x) \in Pol_2[n, x] \ : \ a(\alpha) = 0\}$$

con α elemento primitivo di $GF(2^m)$. Se $\mathbf{y} = \mathbf{a} + \mathbf{j}$ è la parola ottenuta modificando la $j - esima$ componente di una parola $\mathbf{a} \in Ham(m, 2)$, essendo $a(\alpha) = 0$, risulta

$$y(x) = a(x) + x^j \quad \text{e} \quad y(\alpha) = \alpha^j.$$

Con un canale di trasmissione binario, che commette non più di un errore sulle parole di lunghezza $n = 2^m - 1$ e che usa $Ham(m, 2)$ come codice ciclico, si può usare il seguente algoritmo di decodifica, ove $y(x)$ è la parola ricevuta e $z(x)$ la decodifica di $y(x)$:

primo passo: Calcolare $y(\alpha)$.

secondo passo: Se $y(\alpha) = 0$, si ponga $\mathbf{z} = \mathbf{y}$.

terzo passo: Se $y(\alpha) = \alpha^j \neq \mathbf{0}$, si ponga

$$z(x) = y(x) + x^j.$$

5. BCH codici binari $2-$correttori

indice

Una rappresentazione di $Ham(m, 2)$

- Identifichiamo lo spazio vettoriale Z_2^m con il campo di Galois $GF(2^m)$ d'ordine 2^m e sia α un elemento primitivo di $GF(2^m)$, cioè un generatore del gruppo (ciclico) moltiplicativo del campo. Allora abbiamo

$$Z_2^m = GF(2^m) = \{0, 1, \alpha, \alpha^2, ..., \alpha^{2^m-2}\}$$

e l'insieme

$$B = \{1, \alpha, \alpha^2, ..., \alpha^{m-1}\}$$

è una base ordinata di Z_2^m. Ogni potenza di α può identificarsi con l'$m-$pla delle sue componenti rispetto a B.

- Abbiamo precedentemente costruito una matrice di controllo $H_{m,2}$ del codice di Hamming $Ham(m, 2)$ scegliendo come $j-$esima colonna la rappresentazione binaria dell'intero j. Ora, usando la base B, è possibile costruire $H_{m,2}$ identificando le sue colonne con le componenti in B delle potenze di α. Possiamo, quindi, scrivere in forma compatta ($n = 2^m - 1$)

$$H_{m,2} = [1\ \alpha\ \alpha^2\ \ldots\ \alpha^{n-1}].$$

Consideriamo $GF(2^3) = \{a_o + a_1\alpha + a_2\alpha^2 \ : \ a_o, a_1, a_2 \in Z_2\}$,
con α radice del polinomio irriducibile $x^3 + x + 1$. L'elemento α risulta un elemento primitivo di $GF(2^3)$ e quindi

$$GF(2^3) = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}.$$

Dall'essere $\alpha^3 = 1 + \alpha$, risulta $\alpha^4 = \alpha + \alpha^2$, $\alpha^5 = 1 + \alpha + \alpha^2$, $\alpha^6 = 1 + \alpha^2$.
Una base di $GF(2^3)$ su Z_2 è $\{1, \alpha, \alpha^2\}$. Una matrice di controllo di $Ham(3, 2)$ è

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Un'altra matrice di controllo di $Ham(3, 2)$ è

$$[1 \ \alpha \ \alpha^2 \ \alpha^3 \ \alpha^4 \ \alpha^5 \ \alpha^6] = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

PROPOSIZIONE 404

Sia α un elemento primitivo di $GF(2^m)$, $m \geq 4$, e si ponga $n = 2^m - 1$. La matrice

$$H'_m = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^m-2} \\ 1 & \alpha^3 & (\alpha^2)^3 & \cdots & (\alpha^{2^m-2})^3 \end{bmatrix},$$

ove ogni elemento indica la corrispondente $m-$pla binaria, è la matrice controllo di parità di un $[n, n-2m]-$codice ciclico $BCH(2, m)$ con polinomio generatore $g(x) = m_\alpha(x)m_{\alpha^3}(x)$.

DIMOSTRAZIONE 405

Una parola $\mathbf{c} = (c_o, c_1, \ldots, c_{n-1})$ di lunghezza $n = 2^m - 1$ appartiene a $BCH(2, m)$ se, e solo se, $\mathbf{c}{H'_m}^t = \mathbf{0}$. Questo significa che il polinomio

$$c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$$

appartiene a $C(x)$ se, e solo se,

$$c(\alpha) = \sum_{j=0}^{n-1} c_j \alpha^j = 0 \quad \text{e} \quad c(\alpha^3) = \sum_{j=0}^{n-1} c_j \alpha^{3j} = 0,$$

cioè se, e solo se, $m_\alpha(x)$ e $m_{\alpha^3}(x)$ sono divisori di $c(x)$. Questo significa che $BCH(2, m)$ è l'ideale intersezione di quelli generati da $m_\alpha(x)$ e $m_{\alpha^3}(x)$ e, quindi, è generato dal loro minimo comune multiplo $g(x)$. D'altra parte, $m_\alpha(x)$ e $m_{\alpha^3}(x)$ sono irriducibili e distinti tra loro e quindi $g(x) = m_\alpha(x) m_{\alpha^3}(x)$ è il polinomio generatore di $BCH(2, m)$.

PROPOSIZIONE 406

Il codice $C = BCH(2, m)$ avente come matrice di controllo

$$H' = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-2} \\ 1 & \alpha^3 & (\alpha^2)^3 & \cdots & (\alpha^{n-2})^3 \end{bmatrix},$$

ove ogni elemento indica la corrispondente $m-$pla binaria, ha distanza minima 5, risulta cioè $2-$correttore.

DIMOSTRAZIONE 407

Siano $\mathbf{a} \in C$ e $\mathbf{e} = (0, \ldots, 1, \ldots, 1, \ldots, 0)$ la parola che presenta 1 in due posizioni i e j e 0 nelle rimanenti. Posto $\mathbf{b} = \mathbf{a} + \mathbf{e}$, poniamo

$$S(\mathbf{b}) = \mathbf{b}H'^t = \mathbf{a}H'^t + \mathbf{e}H'^t = \begin{bmatrix} \alpha^i + \alpha^j \\ (\alpha^i)^3 + (\alpha^j)^3 \end{bmatrix} = \begin{bmatrix} z_1 \\ z_2 \end{bmatrix},$$

da cui $\alpha^i + \alpha^j = z_1$ e $(\alpha^i)^3 + (\alpha^j)^3 = z_2$. Allora, da

$$z_2 = (\alpha^i + \alpha^j)(\alpha^{2i} + \alpha^i\alpha^j + \alpha^{2j}) = z_1(z_1^2 + \alpha^i\alpha^j), \text{ ricaviamo } \alpha^i\alpha^j = z_1^2 + \frac{z_2}{z_1}$$

e, di conseguenza, α^i e α^j sono le due radici dell'equazione

$$X^2 + z_1X + z_1^2 + \frac{z_2}{z_1} = 0. \tag{55}$$

Così, la conoscenza di $S(\mathbf{b})$ permette di trovare le due posizioni i e j in cui vi sono errori.

DEFINIZIONE 408

Il codice $BCH(2, m)$ definito nella prop.406 si chiama *BCH codice binario 2−correttore* e il polinomio a primo membro della (55) *locatore degli errori di C*.

OSSERVAZIONE 409

La dimostrazione della precedente proposizione evidenzia che, se si vogliono scoprire due errori su una parola del BCH codice binario $BCH(2, m)$, bisogna risolvere l'equazione (55) nel campo di Galois $GF(2^m)$. Si osservi che, in questo caso, la ben nota formula per le soluzioni di un'equazione algebrica di secondo grado perde di significato perché il campo $GF(2^m)$ ha caratteristica 2. Esistono, comunque, altri algoritmi per la risoluzione di questa equazione.

Schema di decodifica di $BCH(2, m)$

passo 1. Si calcola la sindrome $S(\mathbf{b}) = (z_1 \ z_2)^t$ della parola ricevuta $\mathbf{b}$.
passo 2. Se $z_1 = z_2 = 0$, in $\mathbf{b}$ non vi sono errori.
passo 3. Se $z_1 = \alpha^i \neq 0\,,\ z_2 = z_1^3$, allora $S(\mathbf{b})$ è uguale alla colonna $i-$esima di H' e c'è un errore nella posizione i.
passo 4. Se $z_1 \neq 0\,,\ z_2 \neq z_1^3$, allora $S(\mathbf{b}) \neq 0$ e $\mathbf{b}$ presenta almeno due errori:
• se il locatore degli errori ha due radici distinte α^i e α^j, abbiamo esattamente due errori nelle posizioni i e j,
• se il locatore degli errori non ha radici, abbiamo più di due errori.
passo 5. Se $z_1 = 0\,,\ z_2 \neq 0$, allora ci sono più di due errori (in questo caso è $S(\mathbf{b}) \neq \mathbf{0}$ e non può presentarsi un solo errore, altrimenti sarebbe $z_2 = z_1^3$, nè due soli errori, altrimenti avremmo $\alpha^i + \alpha^j = 0$ e due colonne di H' sarebbero uguali, cosa non possibile per costruzione).

Esempio: $BCH(2, 16)$

Consideriamo $GF(2^4) = \{a_o + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \ : \ a_o, a_1, a_2, a_3 \in Z_2\}$, con α radice del polinomio irriducibile x^4+x+1. L'elemento α risulta un elemento primitivo di $GF(2^4)$ e quindi $GF(2^4) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$. Risulta

$$\alpha^5 = \alpha + \alpha^2, \ \alpha^6 = \alpha^2 + \alpha^3, \ \alpha^7 = 1 + \alpha + \alpha^3 \, \alpha^8 = 1 + \alpha^2, \ \alpha^9 = \alpha + \alpha^3,$$

$$\alpha^{10} = 1 + \alpha + \alpha^2, \ \alpha^{11} = \alpha + \alpha^2 + \alpha^3,$$

$$\alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3, \ \alpha^{13} = 1 + \alpha^2 + \alpha^3, \ \alpha^{14} = 1 + \alpha^3.$$

La matrice di controllo di $BCH(2, 16)$ è

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

PARTE 5

CODICI LINEARI E PIANI FINITI

1. Generalità sui piani proiettivi

indice

a Sia $\pi = (\mathcal{P}, \mathcal{L})$ una coppia costituita da un insieme non vuoto $\mathcal{P}$ e da una famiglia $\mathcal{L}$ di sottoinsiemi di $\mathcal{P}$. Gli elementi di $\mathcal{P}$ e di $\mathcal{L}$ si chiamano rispettivamente *punti* e *rette*.

DEFINIZIONE 410

L'insieme di tutte le rette per un fissato punto P si dice *fascio di rette* di centro P. Un punto e una retta che si appartengono si dicono anche *incidenti*.

DEFINIZIONE 411

La coppia $\pi = (\mathcal{P}, \mathcal{L})$ prende il nome di **piano proiettivo** se sono verificate le seguenti proprietà:

$(PP)_1$ due punti distinti appartengono ad un'unica retta;

$(PP)_2$ due rette distinte hanno esattamente un punto in comune;

$(PP)_3$ esistono quattro punti a tre a tre non appartenenti ad una stessa retta (non allineati).

DEFINIZIONE 412

Un *isomorfismo*, o *collineazione*, fra due piani proiettivi $\pi = (\mathcal{P}, \mathcal{L})$ e $\pi' = (\mathcal{P}', \mathcal{L}')$ è una biiezione tra $\mathcal{P}$ e $\mathcal{P}'$ che trasforma rette in rette insieme all'inversa.

OSSERVAZIONE 413

Tutte le collineazioni di un piano proiettivo π in sè formano un gruppo $G(\pi)$. Un piano proiettivo π si studia a meno di collineazioni; si studiano, cioè, le proprietà di π invarianti rispetto al gruppo delle collineazioni $G(\pi)$.

RISULTATO 414

In un piano proiettivo $\pi = (\mathcal{P}, \mathcal{L})$ valgono le seguenti proprietà:

(i) *due rette sono equipotenti;*

(ii) *una retta e un fascio di rette sono equipotenti;*

(iii) *due fasci di rette sono equipotenti;*

(iv) *ogni retta contiene almeno tre punti.*

DEFINIZIONE 415

Sia $\pi = (\mathcal{P}, \mathcal{L})$ un piano proiettivo e denotiamo con $\mathcal{P}^*$ l'insieme dei fasci di rette di π. La coppia $\pi^* = (\mathcal{L}, \mathcal{P}^*)$ è ancora un piano proiettivo, che si chiama il duale di π.

ESERCIZIO 416

Provare che il duale del duale di un piano proiettivo π è isomorfo a π.

ESEMPIO 417

Sia $V = V_3$ uno spazio vettoriale di dimensione 3 su un campo F.

- Denotiamo con $\mathcal{P} = \mathcal{P}(V)$ l'insieme dei sottospazi vettoriali di dimensione 1 di V, che chiameremo *punti* di $\mathcal{P}$.
- Per ogni sottospazio W di V di dimensione 2, denotiamo con $[W]$ il sottoinsieme di $\mathcal{P}$ costituito dai sottospazi 1−dimensionali di V contenuti in W; un insieme di questo tipo prende il nome di *retta* di $\mathcal{P}$.

Allora, denotato con $\mathcal{L}$ l'insieme delle rette di $\mathcal{P}$, la coppia $PG(V) = (\mathcal{P}, \mathcal{L})$ risulta un piano proiettivo che si dice *piano proiettivo associato a V*.

ESERCIZIO 418

Provare che piani proiettivi associati a spazi vettoriali 3−dimensionali sullo stesso campo sono fra loro isomorfi.

DEFINIZIONE 419

Quando è $V = F^3$, il piano $PG(V)$ si denota con $PG(2, F)$ e si chiama *piano proiettivo (numerico) sul campo F*. Un piano proiettivo isomorfo a $PG(2, F)$ si dice *coordinabile* su F.

Se $\mathbf{a}$ è un vettore non nullo di $V = F^3$, denoteremo con

$$< \mathbf{a} > = \{\lambda \mathbf{a} \quad : \quad \lambda \in F\}$$

il sottospazio di V generato da $\mathbf{a}$ e con $[\mathbf{a}]$ il punto di $PG(V)$ corrispondente ad $< \mathbf{a} >$. Risulta:

$$[\mathbf{a}] \neq [\mathbf{b}] \quad \Leftrightarrow \quad \mathbf{a}, \mathbf{b} \text{ indipendenti (non proporzionali).}$$

OSSERVAZIONE 420

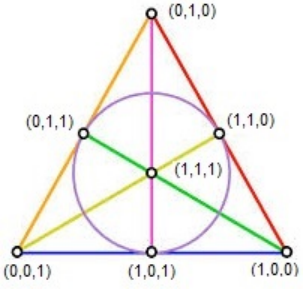
Se $\mathbf{a} = (a_0, a_1, a_2)$ è un vettore non nullo di F^3, il punto $[a] \in PG(2, F)$ resta individuato da una qualsiasi terna $(\lambda a_0, \lambda a_1, \lambda a_2)$, con $\lambda \neq 0$. Tali terne prendono il nome di *coordinate proiettive* (omogenee) del punto $[\mathbf{a}]$. Le rette del piano $PG(2, F)$ si rappresentano mediante equazioni lineari omogenee, cioè del tipo $ax + by + ct = 0$. In particolare, se

$$\mathbf{a} = (a_0, a_1, a_2), \mathbf{b} = (b_0, b_1, b_2) \in F^3,$$

sono due vettori indipendenti, la retta per i punti $[\mathbf{a}], [\mathbf{b}]$ ha equazione:

$$det \begin{bmatrix} x & y & t \\ a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \end{bmatrix} = 0$$

Il piano di Fano $PG(2,2)$



PG(2,2)

Le rette di $PG(2,2)$

equazione	*punti*
$x = 0$	$(0,0,1),(0,1,1),(0,1,0)$
$y = 0$	$(0,0,1),(1,0,1),(1,0,0)$
$t = 0$	$(1,0,0),(1,1,0),(0,1,0)$
$x + y = 0$	$(0,0,1),(1,1,1),(1,1,0)$
$y + t = 0$	$(1,0,0),(1,1,1),(0,1,1)$
$x + t = 0$	$(1,0,1),(1,1,1),(0,1,0)$
$x + y + t = 0$	$(1,0,1),(1,1,0),(0,1,1)$

Sia $A \in GL(3, F)$ e sia L l'automorfismo di F^3 di equazione

$$\begin{pmatrix} x'_0 \\ x'_1 \\ x'_2 \end{pmatrix} = A \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}, \tag{56}$$

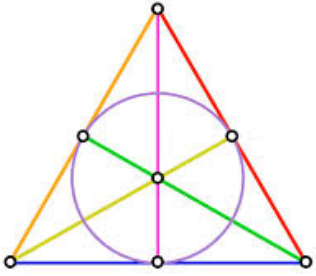
ove (x_i) e (x'_i) rappresentano rispettivamente un generico vettore $\mathbf{x}$ e la sua immagine $L(\mathbf{x})$. Ricordiamo che le colonne di A sono ordinatamente uguali alle componenti dei vettori

$$L(1, 0, 0), L(0, 1, 0), L(0, 0, 1).$$

DEFINIZIONE 421

La (56) definisce una collineazione σ_L di $PG(2, F)$ in sè, che prende il nome di *proiettività.* Le proiettività di $PG(2, F)$ formano un gruppo. La *geometria proiettiva* di $PG(2, F)$ è lo studio delle sue proprietà invarianti rispetto al gruppo delle proiettività.

2. Piani proiettivi finiti



indice

Ordine di un piano proiettivo finito

DEFINIZIONE 422

Un piano proiettivo si dice *finito* se è finito l'insieme dei suoi punti. In questo caso, se $n+1$ è il numero dei punti di una retta, l'intero n si dice *ordine* del piano

PROPOSIZIONE 423

Se $\pi = (\mathcal{P}, \mathcal{L})$ è un piano proiettivo finito d'ordine n, risulta

$$|\mathcal{P}| = |\mathcal{L}| = n^2 + n + 1.$$

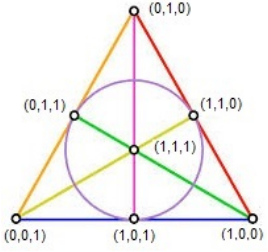
DIMOSTRAZIONE 424

Le rette per un punto P sono $n+1$, ciascuna di essa ha $n+1$ punti e a due a due s'intersecano nel punto P. Tali rette, private del punto P, costituiscono una partizione di $\mathcal{P} \setminus \{P\}$ e, quindi,

$$|\mathcal{P}| = n(n+1) + 1 = n^2 + n + 1\,.$$

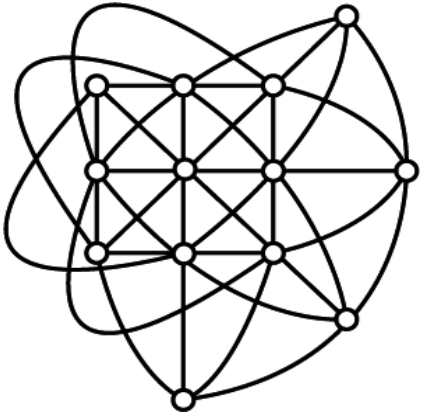
ESERCIZIO 425

Provare che ogni piano proiettivo finito d'ordine 2 è isomorfo al piano di Fano $PG(2,2)$.

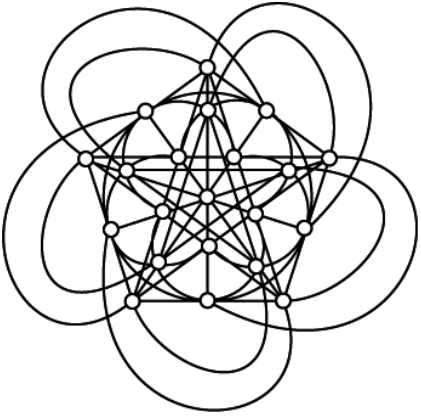


OSSERVAZIONE 426

Il piano proiettivo $PG(2, F_q)$ sul campo di Galois F_q, che si denota con $PG(2, q)$, è un piano proiettivo finito il cui ordine è q.
Ne segue che *esiste almeno un piano proiettivo d'ordine una qualunque potenza di un numero primo*.



$PG(2,3)$



$PG(2,4)$

Possibili ordini dei piani proiettivi finiti

OSSERVAZIONE 427

- Al momento sono note molte classi di piani proiettivi d'ordine $q = p^h > 8$, p primo e $h > 1$, e non isomorfi a $PG(2, q)$.
- Non è ancora noto se esistano o meno piani proiettivi finiti il cui ordine non sia la potenza di un primo.
- Non è ancora noto se esistano o meno piani proiettivi finiti d'ordine primo p non isomorfi a $PG(2, p)$.

TEOREMA 428

Esiste un piano proiettivo d'ordine $n > 2$ se, e solo se, esistono $n - 1$ quadrati latini mutuamente ortogonali.

OSSERVAZIONE 429

Sappiamo che non esistono due quadrati latini ortogonali d'ordine 6. Ne segue che non esiste un piano proiettivo finito d'ordine 6.

Possibili ordini dei piani proiettivi finiti

TEOREMA (R.H.Bruck - H.J.Ryser) 430

Se esiste un piano proiettivo d'ordine $n \equiv 1, 2 (mod\, 4)$, *allora n deve necessariamente essere la somma di due quadrati interi.*

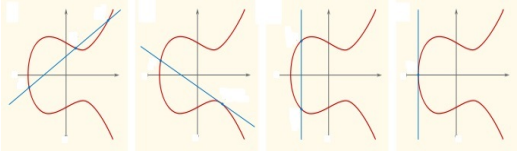
OSSERVAZIONE 431

- Esistono infiniti interi che, in forza del teorema di Bruck-Ryser, non possono essere ordini di piani proiettivi. Per esempio, il numero di tali interi minori di 2000 è 558 e quelli minori di cento sono: 6, 14, 21, 22, 30, 33, 38, 42, 46, 54, 57, 62, 66, 69, 70, 77, 78, 86, 93, 94.
- I primi interi non esclusi dal teorema di Bruck-Ryser sono $n = 10$ e $n = 12$.
  Nel caso **n=10** il problema è stato risolto in senso negativo nel 1989 da *C.W.Lam, S.Swiercz e L.Thiel,* mediante *la teoria dei codici lineari* e l'uso di elaboratori elettronici. Sarebbe interessante *trovare una dimostrazione della non esistenza del piano d'ordine dieci senza l'uso di strumenti di calcolo.*
  Per **n=12** il problema è ancora completamente aperto.

PARTE 6

CODICI LINEARI E CRITTOGRAFIA

1. Richiami e preliminari



indice

AVVISO 432

Qui e nel seguito, parlando in modo informale, attribuiremo gli aggettivi ”facile” e ”buono” a problemi e algoritmi che possano essere risolti in tempo polinomiale con l’ausilio di un computer.

In modo informale, un algoritmo è considerato in tempo polinomiale se il suo tempo di esecuzione $T(n)$ è limitato superiormente da un’espressione polinomiale nella dimensione n dell’input per l’algoritmo, cioè, $T(n) = O(n^h)$ per una qualche costante h.

Ricordiamo che:

- la classe dei problemi risolubili con algoritmi polinomiali si denota con **P** (polynomial time);
- la classe dei problemi per i quali ogni soluzione può essere verificata con algoritmi polinomiali si denona con **NP** (nondeterministic polynomial time);
- risulta $\mathbf{P} \subseteq \mathbf{NP}$ e una famosa congettura vuole che sia $\mathbf{P} = \mathbf{NP}$.

ESEMPIO 433

Verificare se un intero è fattore di un altro è un problema di **P**. Fattorizzare un intero è un problema in **NP**. È stato provato solo nel 2002 che il problema di verificare se un intero è primo (noto in letteratura come PRIMES) appartiene a **P**.

IL NUOVO TEST DI PRIMALITA'

1. input: integer $n > 1$
2. if (n has the form a^b with $b > 1$)
   then output COMPOSITE
3. $r := 2$
4. while ($r < n$)
   {
   if ($gcd(n, r)$ is not 1)
   then output COMPOSITE
   if (r is prime greater than 2) then {
   let q be the largest factor of $r-1$
   if ($q > 4sqrt(r)\log n$) and ($n^{(r-1)/q}$ is not 1 (mod r)) then break }
   $r := r+1$
   }
5. for $a = 1$ to $2sqrt(r)\log n$
   {
   if ($(x-a)^n$ is not (x^n-a) (mod x^r-1, n))
   then output COMPOSITE
   }
   output PRIME;

Gli autori del teorema "PRIMES IS IN P"

da sinistra a destra:
Nitin Saxena,
Neeraj Kayal
e Manindra Agarwal

Sia F un campo. Il piano affine $AG(2, F)$ sul campo F ha per punti gli elementi dello spazio vettoriale F^2 e per rette i laterali dei sottospazi vettoriali di dimensione 1 di F^2.
Valgono le seguenti proprietà:

- due punti distinti appartengono ad un'unica retta;
- fissati una retta ℓ e un punto P, esiste un'unica retta m per P parallela ad ℓ (due rette ℓ, m si dicono parallele se non hanno punti in comune o $\ell = m$);
- ogni retta ℓ è rappresentata da un'equazione lineare $ax + by + c = 0$, con $(a, b) \neq (0, 0)$, cioè

$$\ell = \{(\overline{x}, \overline{y}) \in F^2 \ : \ a\overline{x} + b\overline{y} + c = 0\}$$

Sia $AG(2, F)$ il piano affine su un campo F.

- Se $P = (a, b)$ è un punto ed ℓ la retta di equazione $ax + by + c = 0$, diremo (a, b) e (a, b, c) coordinate di P ed ℓ, rispettivamente.
- Il parallelismo fra rette è una relazione di equivalenza le cui classi di equivalenza si chiamano direzioni o punti impropri (in contrapposizione ai punti di $AG(2, q)$, che si dicono propri).
- Fissata una direzione δ e un punto proprio P esiste un'unica retta per P con direzione δ.

NOTAZIONE 434

Denotiamo con **O** *la direzione della retta* $x = 0$ *(asse y).*

Piano affine su un campo finito

Il piano affine su un campo finito F_q, con q elementi si denota con $AG(2, q)$ e verifica le seguenti proprietà:

- il numero dei suoi punti è q^2;
- il numero delle sue rette è $q^2 + q$;
- il numero di punti di una retta è q;
- il numero delle rette per un punto è $q + 1$.

DEFINIZIONE 435

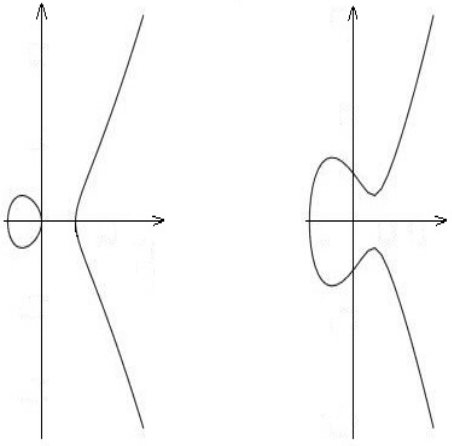
Una curva ellittica $E = E(a, b, c, d, e)$ su un campo F è una curva di $AG(2, F)$ di terzo grado e non singolare avente equazione del tipo

$$f(x, y) = y^2 + axy + by - x^3 - cx^2 - dx - e = 0\,, \quad a, b, c, d, e \in F\,. \quad (57)$$

In altre parole, E è il luogo dei punti di $AG(2, F)$ le cui coordinate verificano un'equazione algebrica del tipo (57), per cui il sistema

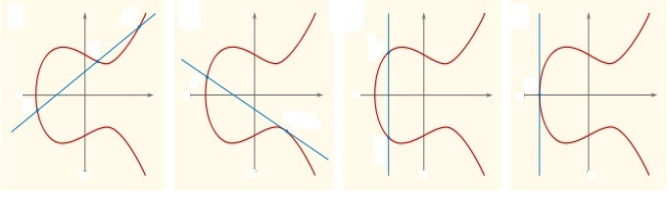
$$\frac{\partial f}{\partial x} = ay - 3x^2 - 2cx - d = 0$$
$$\frac{\partial f}{\partial y} = 2y + ax + b = 0$$

non ammette soluzioni.



Se E è una curva ellittica sul campo F, valgono le seguenti proprietà:

1. Ogni retta non verticale (non parallela a $x = 0$) con più di un punto su E interseca E in esattamente tre punti (contati con la loro molteplicità).
2. Ogni retta verticale (parallela a $x = 0$) con più di un punto su E interseca E in esattamente due punti (contati con la loro molteplicità).



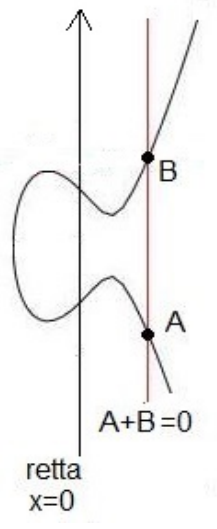
Gruppo abeliano associato ad una curva ellittica E

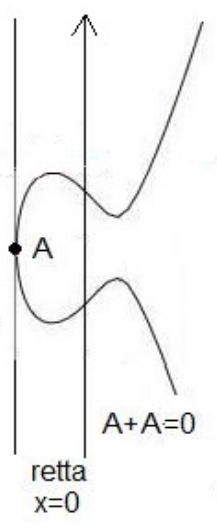
su un campo F

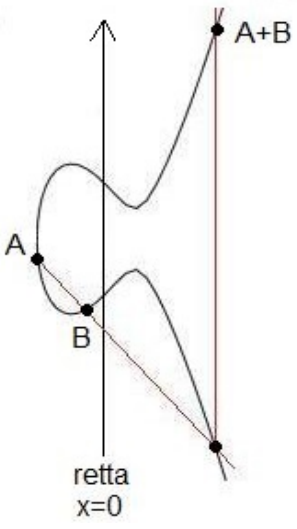
Si ponga $G(E) = E \cup \{\mathbf{O}\}$. Allora su $G(E)$ resta definito un gruppo abeliano additivo (gruppo associato ad E), con elemento neutro $\{\mathbf{O}\}$, nel seguente modo:

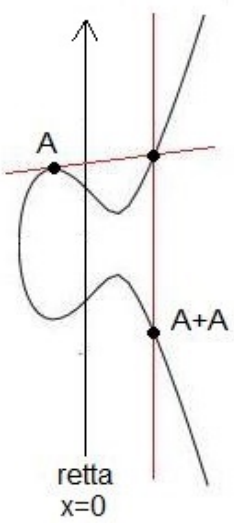
- Per ogni punto $A \in E$, si pone $\mathbf{O} + \mathbf{O} = \mathbf{O}$, $\mathbf{O} + A = A + \mathbf{O} = A$.
- Per ogni due punti $A, B \in E$,
  1. se $A \neq B$ e la retta per A, B è parallela all'asse y, si pone $A + B = \mathbf{O}$;
  2. se $A = B$ e la retta tangente in A ad E è parallela all'asse y, si pone $A + A = \mathbf{O}$;
  3. se $A \neq B$ e la retta ℓ per A, B non è parallela all'asse y, si considera il terzo punto C che ℓ ha in comune con $G(E)$, si considera la retta m per C parallela all'asse y (cioè, con direzione $\mathbf{O}$), si pone $A + B$ uguale all'unico punto proprio diverso da C che la retta m ha in comune con $G(E)$;
  4. se $A = B$ e la tangente ℓ in A ad E non è parallela all'asse y, si considera il terzo punto C che ℓ ha in comune con $G(E)$, si considera la retta m per C parallela all'asse y, si pone $A + B$ uguale all'unico punto proprio diverso da C che la retta m ha in comune con $G(E)$.

Gruppo abeliano associato ad una curva ellittica









2. Introduzione alla crittografia

indice

Considerazioni preliminari

- INTERNET è oggi il mezzo più semplice, comodo e veloce per trasmettere informazioni.
- Un pirata informatico (hacker) non ha molte difficoltà nell'intercettare, leggere e, a volte, modificare i dati trasmessi.
- Abbiamo problemi seri quando i dati intercettati contengono informazioni riservate come numeri di carte di credito, password e ogni altro tipo di "messaggio segreto".
- Al momento non sono immaginabili nuove tecnologie che impediscano l'intercettazione di informazioni riservate.

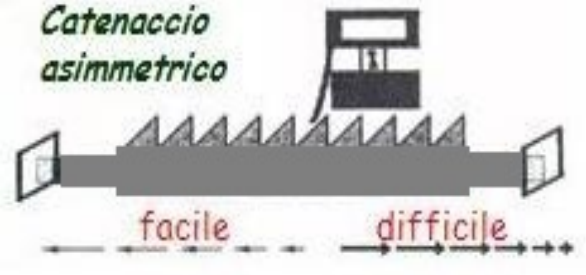
MORALE 1

Non possiamo difenderci usando l'hardware?
Cerchiamo di farlo usando il software!

Come si nascondono le informazioni riservate?

- Bisogna trasformare ”facilmente” (cifrare) il messaggio originale (testo in chiaro) in uno che apparentemente non abbia alcun senso (testo cifrato).
- Il testo cifrato deve poter essere ”facilmente” tradotto (decifrato) nel messaggio originale solo con l'uso di una speciale informazione (chiave).
- Tali operazioni si possono fare utilizzando le funzioni unidirezionali. Queste, detto in modo informale, sono funzioni biunivoche ”facilmente calcolabili”, per le quali è praticamente impossibile il calcolo dell'inversa senza la conoscenza di un'opportuna informazione (chiave).

Una versione hardware delle funzioni unidirezionali



Un esempio di funzione unidirezionale: il prodotto di due primi

OSSERVAZIONE 436

- Moltiplicare due interi è ”facile”.
- Dividere un intero per un’altro è ”facile”.
- Fattorizzare in primi un intero è ”difficile”.

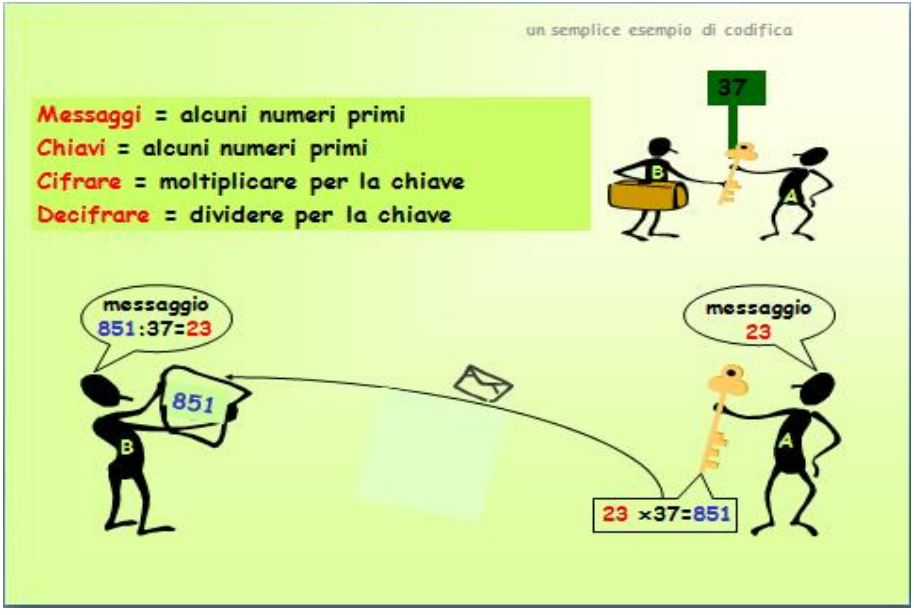
RISULTATO 437

La funzione

$$\{p, q\} \rightarrow pq\,,$$

che ad ogni due primi $\{p, q\}$ *associa il loro prodotto* pq*, è unidirezionale.*

Un esempio di codifica col prodotto di primi



Un secondo esempio di funzione unidirezionale: il logaritmo discreto

OSSERVAZIONE 438

Siano G un gruppo ciclico finito d'ordine N e g un suo generatore.

- È "facile" calcolare la potenza $x = g^k$, con k intero $0 < k < N$.
- Noto $b = g^k$, è "difficile" calcolare $k = \log_g x$ (il logaritmo discreto di b).

RISULTATO 439

La funzione

$$k \rightarrow g^k ,$$

che ad ogni intero k, $0 < k < N$, associa l'elemento g^k di G, è unidirezionale.

Un esempio di algoritmo per lo scambio di una chiave segreta

Siano G un gruppo ciclico finito e g un suo generatore.

- Ogni utente A sceglie in segreto un intero $s(A)$.
- La chiave segreta relativa a due utenti A e B è

$$s(A,B) = g^{s(A)s(B)}$$

e può essere scambiata in modo riservato utilizzando il seguente algoritmo [algoritmo DH (Diffie-Hellman)]:

passo 1: A calcola $g^{s(A)}$ e lo invia a B, analogamente B calcola $g^{s(B)}$ e lo invia ad A;

passo 2: A calcola $(g^{s(B)})^{s(A)} = s(A,B)$ e, analogamente, B calcola $(g^{s(A)})^{s(B)} = s(A,B)$.

OSSERVAZIONE 440

Alla fine di questa procedura l'utente A conosce $s(B)$ $(= \frac{s(A,B)}{s(A)})$ e l'utente B conosce $s(A)$ $(= \frac{s(A,B)}{s(B)})$.

DEFINIZIONE 441

Un crittosistema simmetrico è una quaterna

$$(D, M, K, \{f_m \ : \ m \in K\})$$

ove

- D, M e K sono insiemi (l'insieme dei *messaggi in chiaro*, l'insieme dei *messaggi cifrati* e l'insieme delle *chiavi*, rispettivamente).
- $f_m : D \to K$ è una funzione unidirezionale tra D e $f_m(D)$ (*codifica relativa alla chiave m*).

OSSERVAZIONE 442

Nella crittografia simmetrica il mittente (per cifrare) e il destinatario (per decifrare) usano la stessa chiave segreta (nel senso che le due chiavi possono facilmente ricavarsi l'una

Alcuni inconvenienti della crittografia simmetrica

La crittografia simmetrica presenta tre grossi inconvenienti:

1. mittente e destinatario devono scambiarsi la chiave prima dell'inizio delle comunicazioni;
2. una buona chiave è molto lunga e vi sono seri problemi di sicurezza per la sua trasmissione;
3. in un sistema con "molti" utenti il numero di chiavi da scambiarsi a coppie è così alto che la gestione di questa fase diventa abbastanza complicata.

Importanza delle chiavi

La crittografia moderna dà estrema importanza alle chiavi. Essa, infatti, basa la sua efficienza sul seguente principio.

IL PRINCIPIO DI KERCKOFFS 443

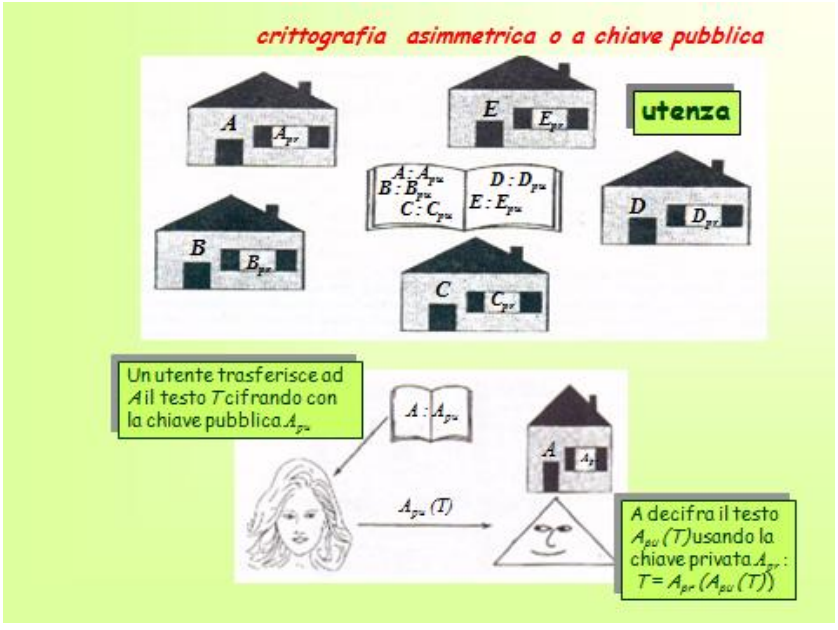
La sicurezza di un crittosistema non dipende dalla segretezza e dalla complessità degli algoritmi per cifrare e decifrare ma soltanto dalla segretezza delle chiavi.

Crittografia asimmetrica o a chiave pubblica

In contrasto con quella simmetrica, la crittografia asimmetrica opera nel modo seguente:

- gli algoritmi per cifrare e decifrare sono di dominio pubblico e ogni utente A genera in privato una propria coppia di chiavi (A_{pu}, A_{pr});
- la chiave A_{pu} serve per cifrare i messaggi da inviare ad A ed è pubblica, la chiave A_{pr} serve per decifrare ed è nota solo ad A;
- un messaggio T cifrato con la chiave (pubblica di A) A_{pu} può essere decifrato solo con la chiave (privata di A) A_{pr}, cioè $A_{pr}(A_{pu}(T)) = T$;
- per inviare un messaggio all'utente A bisogna cifrarlo con la chiave (pubblica di A) A_{pu} e il messaggio così cifrato può essere decifrato con la chiave (privata di A) A_{pr} solo da A.

Crittografia asimmetrica o a chiave pubblica



OSSERVAZIONE 444

La crittografia asimmetrica permette una gestione semplice e sicura delle chiavi segrete, in accordo col principio di Kerckoffs:

- ciascun utente genera la propria chiave privata e non deve trasmetterla;
- per le trasmissioni è sufficiente rendere disponibile a tutti solo la chiave pubblica di ciascun utente.

Il crittosistema RSA, il primo a chiave pubblica

(basato sulla difficoltà della fattorizzazione in primi degli interi)

il crittosistema RSA

Nel 1977 tre persone diedero il più spettacolare contributo alla crittografia a chiave pubblica: Ronald Rivest, Adi Shamir e Leonard Adleman … raccolsero la sfida di produrre un crittosistema a chiave pubblica completo. Il lavoro durò alcuni mesi durante i quali Rivest proponeva strade possibili. Adleman le attaccava e Shamir faceva o l'una o l'altra cosa.

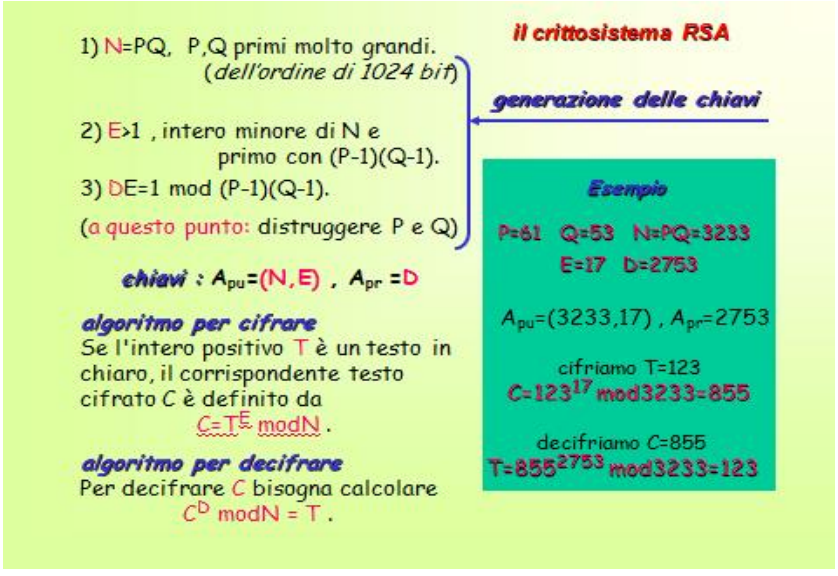
Nel maggio del 1977 essi furono ricompensati dal successo … Avevano scoperto come una semplice parte della teoria classica dei numeri poteva essere usata per risolvere il problema.

[W.Diffie, The first ten years of public-key cryptography, Proceedings of IEEE 76 (5), 1988, 560-577]

http://zoo.cs.yale.edu/classes/cs426/2012/bib/diffie88first.pdf

Il crittosistema RSA

https://it.wikipedia.org/wiki/RSA



La Crittografia da Atbash a RSA

http://www.crittologia.eu

Crittosistema di ElGamal

(basato sulla difficoltà del calcolo del logaritmo discreto)

https://it.wikipedia.org/wiki/ElGamal

Si fissino un gruppo ciclico finito G d'ordine N ed un suo generatore g e si assuma che i messaggi da trasmettere siano gli elementi di G.

- Ogni utente A possiede:
  - una chiave privata costituita da un intero s(A) (scelto in modo riservato da A stesso), $0 < s(a) < N$;
  - una chiave pubblica $p(A)$, costituita dall'elemento $g^{s(A)}$ del gruppo G

Crittosistema di ElGamal

(basato sul problema del calcolo del logaritmo discreto)

- Un utente A che voglia inviare un messaggio $m \in G$ ad un utente B :
  - (1) prende la propria chiave privata $k = s(A)$ e la chiave pubblica $b = p(B) = g^{s(B)}$ di B;
  - (2) codifica il messaggio m con la coppia $(g^k, mb^k) = (\gamma, \delta)$.
- L'utente B decodifica il messaggio cifrato (γ, δ) calcolando

$$\gamma^{-s(B)} \cdot \delta = g^{-ks(B)} \cdot mb^k = g^{-ks(B)} m g^{ks(B)} = m.$$

OSSERVAZIONE 445

Per questo crittosistema sono molto usati i gruppi moltiplicativi dei campi finiti e i sottogruppi ciclici dei gruppi associati a curve ellittiche su un campo finito.

3. Codici lineari e crittosistema di McEliece

Robert McEliece

https://en.wikipedia.org/wiki/Robert_McEliece

indice

Osservazione

L'algoritmo di decodifica più generale di un codice lineare, la *decodifica a sindromi,* non è efficiente. Esistono, però, classi di codici, come quelli binari di Hamming (e altri che non abbiamo studiato), che ammettono degli schemi di decodifica veloci.

Questa osservazione suggerisce la costruzione di crittosistemi a chiave pubblica che usano i codici lineari [R.J.McEliece (1978)].

Una nuova idea

L'idea è quella di usare un codice lineare C con decodifica veloce e di prendere come testi cifrati le parole di C modificate in modo che:

- conoscendo una *chiave* è possibile decifrare usando l'algoritmo veloce di decodifica di C;
- senza la conoscenza della chiave l'unico modo per decifrare è quello di usare la decodifica a sindromi.

Si fissi un $[n, k]-$codice lineare $t-$correttore C con un algoritmo di decodifica veloce e sia G una sua matrice generatrice.

- Ogni utente possiede:
  - una chiave privata costituita da una coppia (S, P), ove S è una matrice binaria casuale $k \times k$ non singolare e P una matrice di permutazione casuale;
  - una chiave pubblica costituita dalla matrice $\overline{G}$ di tipo $k \times n$ definita da

$$\overline{G} = SGP.$$

- Un utente A che voglia inviare un messaggio (binario) $\mathbf{a}$ ad un utente B deve usare il seguente algoritmo:

  (1) Spezza $\mathbf{a}$ in blocchi di lunghezza k e opera separatamente su ciascuno di questi.

  (2) Ogni blocco $\mathbf{x}$ è codificato in una parola $\mathbf{y}$ di lunghezza n mediante la chiave pubblica $\overline{G}$ di B nel seguente modo:

$$\mathbf{y} = \mathbf{x}\overline{G} + \mathbf{e}\,, \tag{58}$$

  ove $\mathbf{e}$ è un vettore casuale di lunghezza n e di peso al più t.

- L'utente B decodifica ogni $\mathbf{y}$ che riceve nel seguente modo:
  (1) Calcola
  $$\overline{\mathbf{y}} = \mathbf{y}P^{-1} = (\mathbf{x}\overline{G}+\mathbf{e})P^{-1} = (\mathbf{x}SGP+\mathbf{e})P^{-1} = \mathbf{x}SG+\mathbf{e}P^{-1}.$$
  (Il vettore $\mathbf{e}P^{-1}$ ha peso al più t e $\mathbf{x}SG \in C$)
  (2) Decodifica $\overline{\mathbf{y}}$ usando l'algoritmo veloce di decodifica di C. In questo modo ottiene $\mathbf{x}S$ perché $\mathbf{e}P^{-1}$ ha peso al più t.
  (3) Calcola $\mathbf{x} = (\mathbf{x}S)S^{-1}$.

OSSERVAZIONE 446

Partendo da un codice lineare, si può costruire un crittosistema (crittosistema di Niederreiter) utilizzando le matrici di controllo, invece delle matrici generatrici, in modo del tutto analogo a quanto fatto con lo schema di McEliece.

Scegliamo C uguale al $[7,4,3]-$ codice binario di Hamming $1-$correttore $Ham(3,2)$ e sia

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}. \text{ Se } S = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}, P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

risulta

$$\overline{G} = SGP = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Se è $\mathbf{x} = (1,1,0,1)$, $\mathbf{e} = (0,0,0,1,0,0)$, risulta

$$\mathbf{y} = \mathbf{x}\overline{G} + \mathbf{e} = (0,1,1,0,0,1,0) + (0,0,0,0,1,0,0) = (0,1,1,0,1,1,0),$$

$$P^{-1} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

e, $\overline{\mathbf{y}} = \mathbf{y}P^{-1} = (1,0,0,0,1,1,1)$. Allora:

$$S(\overline{\mathbf{y}}) = (1,1,1,0) = (7)_2,$$

quindi c'è un errore nella settima posizione di $\overline{\mathbf{y}}$ che è decodificato come $(1,0,0,0,1,1,0)$.

Ne segue che

$$\mathbf{x}S = (1,0,0,0).$$

Concludendo, risulta

$$S^{-1} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

e, quindi,

$$\mathbf{x} = (1,0,0,0)S^{-1} = (1,1,0,1).$$

OSSERVAZIONE 447

Per decifrare un messaggio **y** senza la conoscenza della chiave privata (S, P) si deve usare l'algoritmo di decodifica a sindrome per il codice generato dalle righe della matrice $\overline{G}$ e tale algoritmo, come più volte osservato, non è efficiente.

Per il crittosistema di McEliece si utilizzano dei codici lineari (codici di Goppa) che si costruiscono mediante curve algebriche (in particolare curve ellittiche) su campi finiti.

In un esempio dato da McEliece, con $n = 1024$ e $t = 50$, bisogna calcolare più di 10^{80} sindromi!

Una curiosità sull'ordine di grandezza di 10^{80}

Stime ragionevoli basate sul numero di galassie esistenti,
sul numero di stelle mediamente presenti in ogni galassia
e sul numero di atomi che mediamente costituiscono una stella
fanno ritenere che
il numero di atomi presenti nell'universo
sia compreso fra 10^{79} **e** 10^{81}.

Sicurezza crittografica e quantum computer

video su "McEliece and Niederreiter Cryptosystems That Resist Quantum Fourier Sampling Attacks"

Attualmente i sistemi crittografici a chiave pubblica più sicuri sono:

(a) i sistemi che si basano sulla non conoscenza di algoritmi efficienti per la scomposizione di un intero in fattori primi e per il calcolo del logaritmo discreto in un gruppo finito (RSA, ElGamal,...);

(b) i sistemi che si basano sulla non conoscenza di algoritmi efficienti per la decodifica a sindromi di codici lineari arbitrari (McEliece, Niederreiter).

È noto che i sistemi di tipo (a) non resistono all'attacco di alcuni algoritmi quantici (che potrebbero girare cioè su un (almeno per il momento ideale) quantum computer), detti di Shor.

Recentemente è stato provato (H.Dinh, C.Moore, A.Russel) che i crittosistemi di McEliece e di Niederreiter, costruiti su particolari codici lineari, sono in grado di resistere agli attacchi degli algoritmi quantici di Shor.

LETTURE CONSIGLIATE

• **L.Berardi**, *Algebra e teoria dei codici correttori*, Collana di matematica e statistica, Franco Angeli Editore, 1994.

• **L.Giuzzi**, *Codici correttori*, Collana UNITEXT, Springer, 2006.

• **R.Hill**, *A First Course in Coding Theory*, Oxford Applied Mathematics and Computing Science Series, Clarendon Press - Oxford, 1990.

indice